

CRN

CHANNELWEB.CO.UK

The true cost of security



Sponsored by





Seeing an impact

Channel players and their customers need to consider not just what a product does, but the impact of how it does it, according to Malcolm Tuck

The arms race between cyber criminals and cyber security vendors has gained pace over the last few years. The level of sophistication employed by both sides has reached new heights, and the trend is set to continue for the foreseeable future.

The traditional considerations for choosing a security solution – whether you are a reseller, MSP or end user – need a new focus.

Clearly, it's very important that high detection rates are a key component in the procurement process decision criteria, but the difference between the major vendors is relatively insignificant. It's not only what the security software does but also how the solution is delivered, performs and maintains that needs to be given more priority. It's also not enough just to consider the capital cost of the licence because this may not be your, or their, largest cost of ownership consideration.

Desktops and laptops are designed to enable end users to do their jobs, not to prevent malware attacks. But we are asking these devices to do more and more in preventing breaches which, invariably, means increases in system resource usage and ultimately slows them down, thereby preventing their original purpose – to support the end user.

As a consequence, subbing out certain processes to cloud sandboxing technology has become more prevalent, delivering an increase of several orders of magnitude: from raw computing power running concurrent machine-learning processes to sophisticated algorithms identifying the latest state-of-the-art malware. Even modern laptops

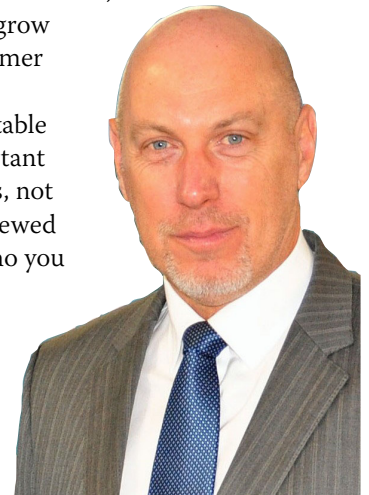
and desktops would be rendered inoperative for weeks, or months, for what these super computers can achieve in just minutes.

That said, you still need the endpoint security to do relatively resource-heavy tasks and this is where the choice of security vendor is key. All things being equal – detection rates, ransomware protection, botnet protection, management console functionality etc – other factors come into play.

As a reseller or MSP, elements such as system impact (how much the security solution slows a machine down), false positives (and remediation thereof) and a total cost of management/ownership directly affect profitability, operational costs, scalability (your ability to grow in this instance) and customer satisfaction/retention.

When considering a suitable security partner, it's important to consider these elements, not just as a spot check, but viewed over a period time – as who you next recommend to your client could have a huge impact on your business for years to come.

*Malcolm Tuck,
managing director of
ESET UK*



Security at all costs

The channel and its customers have long taken into consideration whole-life costs for end user and datacentre hardware. But, as this CRN research report uncovers, the worlds of security and software are often overlooked.

Although we may not always apply the term to the situation in question, the concept of 'total cost of ownership' is one that, for most of us, governs a huge array of decisions in our daily life.

It is an idea that is embedded in our decision to use energy-saving lightbulbs, or buy the bigger bottle of ketchup, as well as in our choice to spend a bit more on a decent winter coat or a pair of headphones that will not pack in after a few months of commuting.

In those everyday instances, we would likely just think of it as value for money – if we thought about it at all.

Many people in the technology industry, however, have given the concept a great deal more consideration.

Thus, the idea of total cost of ownership – which is just as it sounds – represents how much, in total, it will cost an organisation to buy and use a piece of technology. This means not just the initial investment in acquiring the product, but all ongoing expenses from there; including energy usage and performance efficiencies, as well as the cost of downtime, maintenance and, ultimately, upgrade or replacement.

TCO has become a common metric by which hardware products are judged and also marketed. Channel firms and their customers will invariably consider the lifetime costs of an investment in both end user devices and datacentre infrastructure. This is ever-more-so the case in a world where hosted or cloud-based alternatives are on offer.



Despite its integrality to every organisation's IT estate, software is rarely subjected to the same scrutiny. Yet it is through software tools that most of us live much of our lives these days, both at work and in our personal time. And we certainly notice when the applications in question are slow or malfunctioning.

Nowhere is speed and accuracy more important than in cybersecurity. For this report, we surveyed more than 150 senior decision makers at channel firms. Our study quizzed them on their organisation's security business, their view of the threat landscape and the role of total cost of ownership in technology deployments.

Our research first finds that, despite the challenges faced in the past year, VARs' security sales have held up extremely well. When we surveyed them in April 2021, six in ten respondents told us that their revenue from cyber products and services has increased in the past 12 months. More than a quarter indicated that sales have risen by more than 10 per cent. Only about one in 15 channel players, meanwhile, has seen a decline in their security business.

Pierre Louw, UK head of MSP for security vendor ESET, pointed out that this strong performance is a continuation of a trend that has seen the annual value of the UK cybersecurity industry expand 46 per cent since 2017 to £8.3bn in 2020.



If you factor in the potential total cost of ownership – especially with large numbers of endpoints – system impact should be a key consideration. Slower machines are likely to have the knock-on effect of an increased burden on tech support, reduced productivity, and greater, more costly energy usage.

Steve Connolly, ESET

Examining the true cost of security

“The trend continues – the key difference being that end users are now focusing spend and investment towards threat intelligence, monitoring, detection and analysis,” he added.

The last year has been busy not just for the cyber industry, according to Louw, but for those whose threats need to be kept out.

“The threat landscape is fast-changing with new technologies like FinTech, behaviour shifts to home working, and a massive growth in online shopping presenting new opportunities for cybercriminals,” he said. “Just looking at the data from UK police forces, we see that cybercrime overall rose by 19 per cent between January 2020 and January 2021.”

Perhaps the robustness of the security sector can also be attributed to the incessance of the most common threats encountered by end users.

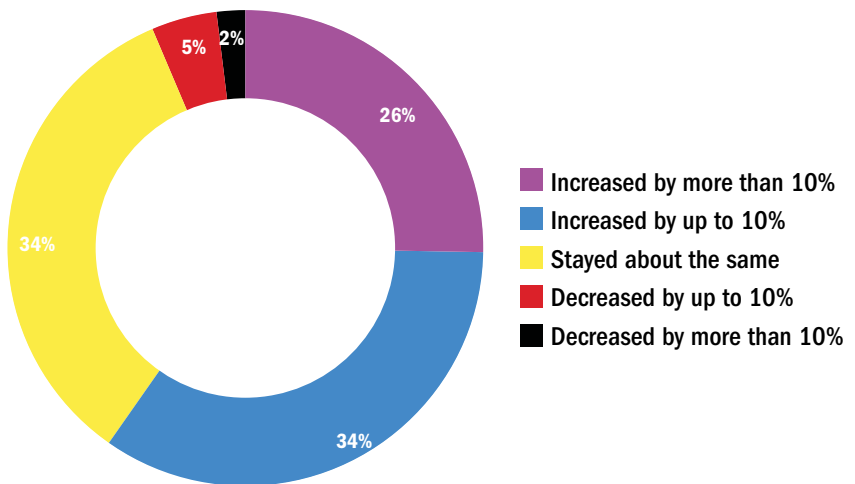
When we asked our channel leaders to rank, from first to last and in order of significance and severity, six major areas of the threat landscape currently facing their customers, we find that the long-standing staples are still posing the biggest challenge.

Top of the pile was phishing attacks; if the maximum possible score – in which all respondents placed it in first place – is pegged at 100, then phishing scored 77.3.

Not far behind were ransomware and malware attacks, on 75.3 and 72.9, respectively.

These familiar foes were some way ahead of newer or more complex dangers. Advanced persistent threats scored 49.1 out of 100 to place fourth on our list, with insider threats on 41.8 and, last of all, cryptojacking attacks on 40.5.

How have your cybersecurity products and services sales changed in the past 12 months?



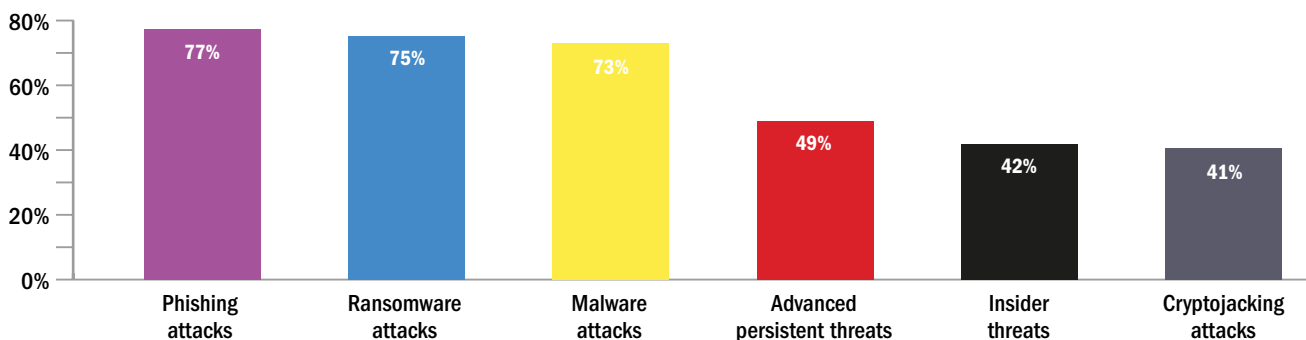
Our study suggests that the dominant dangers are likely to remain so for a while yet, as they pose not only the biggest threats – but the fastest-growing ones.

More than 80 per cent of channel chiefs said that the risks posed to their organisation’s customers by phishing attacks have increased in the past year. Some 42.8 per cent said they have increased ‘greatly’.

For ransomware attacks, upwards of 70 per cent have seen an increase in threat levels, with 25.2 per cent citing a ‘significant’ rise. The third of the big three, malware attacks, posted similar figures of 69.8 and 15.8 per cent, respectively.

Although the vast majority of respondents said the threat level had increased or remained steady for all of our cited security issues, the newer threats are seemingly growing at a slower rate than their more established peers.

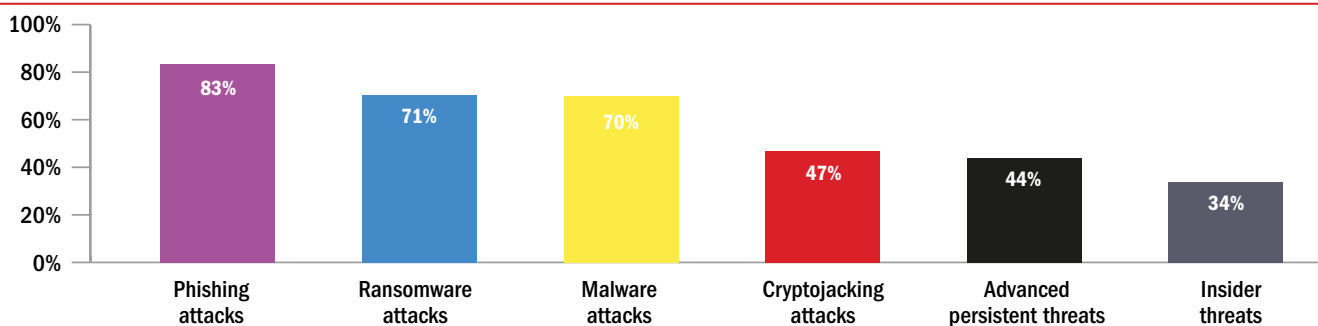
Common threats, ranked by significance and severity of threat posed to end users*



*Comparative to maximum possible score, where maximum possible score is 100

Examining the true cost of security

Proportion of channel leaders that believe the following threats have increased in the past year



For cryptojacking attacks, 46.7 per cent of respondents reported having seen an increase in the scale of the dangers posed in the past year. Some 43.8 and 33.8 per cent said the same of APTs and insider threats, respectively.

A year to remember

We asked our channel chiefs to tell us in more detail about how their view of the cybersecurity landscape – and that of their clients – has changed in the past year.

The most significant difference is the most obvious one, according to our survey respondents: a large number of whom cited mass working from home as the trend that has had the most profound impact.

The potential ramifications of remote working include a proliferation of the number of people who might have access to devices and data, as well as more lax security systems.

“People working remotely on their own devices – possibly shared with other family members – increases the surface area of attack vectors and makes it harder for customers to mitigate all possible threats and risks,” one of our research participants said.

“The number of people working from home has greatly increased and this lessens the security threshold as some are using their home computers which tend to have fewer security controls in place,” another added.

According to one reseller boss, cyberattackers – as they ever do – have adapted their methods and modes of attack in response to the new environment.

“COVID-19 has played a big part in the increase of risk in the threat landscape for our customers,” they said. “There has been a massive increase in attempted ransomware attacks, with a focus on attacking backups – so they can’t restore. Our focus this year has been on securing their backups to prevent any ransomware attacks from taking them offline.”

The dispersal of the workforce has also provided a reminder that an organisation’s people remain the single

biggest – and often most vulnerable – part of the attack surface. “Many of our customers have little IT knowledge and the risk of them opening a malicious attachment or clicking a dodgy link in an email is frighteningly high,” one of our respondents told us. Another said: “Organisations still neglect the element of human error.”



Organisations need constant education of staff to get them to be acutely aware and not trust everything they receive.

Working from home has pushed the trust boundary out even further, so companies need to feel more confident in security solutions.

A number of our research participants cited the need for more – and more comprehensive – training for staff.

One channel leader said that “cyber awareness training is a must for any organisation”.

Another indicated that education and technical defences need to work symbiotically.

“Organisations need constant education of staff to get them to be acutely aware and not trust everything they receive,” they said. “Working from home has pushed the trust boundary out even further, so companies need to feel more confident in security solutions.”

The good news, according to a number of those who took part in our study, is that the pandemic has, in many cases, proven to senior managers the importance of cybersecurity – and the risks of getting it wrong.

“People have definitely become more aware – now up to board level, rather than just IT director level,” one respondent said.

However, as another pointed out, cognisance of a problem is not the same thing as a willingness to spend money to fix it.

“Awareness has increased – especially during the COVID period – but that is not easily translated into investment,” they said.

Totally focused

In recent years, total cost of ownership – encompassing the ongoing costs of factors such as energy usage, maintenance, and downtime – has become an increasingly important consideration during organisations’ procurement of technology products and services.

For end users, minimising TCO is an exercise not just in saving costs, but in achieving operational efficiencies and cutting carbon footprint. For their IT providers, helping them do this is a means to become a more valued partner.

But our survey finds that the extent to which ongoing ownership costs are considered in purchasing decisions varies greatly between different areas of technology.

For end user computing devices, it is a significant consideration in 68.8 per cent of conversations between channel firms and clients. The figure for computing infrastructure – 64.8 per cent – is similarly high. The process of buying cloud and hosting services, on 56 per cent, also takes into account TCO more often than not.

Networks, on 47.2 per cent, and storage hardware, on 44.8 per cent, are next on the list.

But considerations of total cost of ownership are much rarer in the software world.

They are a little more common for security programs, with 42.4 per cent of channel chiefs indicating that their clients account for TCO. But this is still a long way short of core hardware and hosting services.

Enterprise software, on 27.2 per cent, and commodity software, on 11.2 per cent, are even further down the list.

Steve Connolly, head of UK channel marketing at ESET, said that security products and services should firstly be judged by their efficacy in keeping out threats. But a detailed examination of the true costs of performance is also crucial – particularly for larger deployments.

“Software security purchase decisions are quite rightly made on high detection rates, low false positives, scalability, good functionality, easy dashboard usability, good reporting capability and a combination of comparatives websites, supported by experience and peer research,” he said. “However, if you factor in the potential total cost of ownership, especially with large numbers of endpoints, system impact should be a key consideration. Slower machines are likely to have the knock-on effect of an increased burden on tech support, reduced productivity, and greater, more costly energy usage, which in turn even has an environmental impact.

The total cost of ownership becomes especially significant if you are supporting thousands of endpoints. The savings an end user can make by selecting a vendor with a low-system-impact solution could even outweigh the cost of the licence itself.”



False positives lead to wasted time investigating dead ends. A security analyst’s time can be expensive, and that’s time which could be spent on true positives to mitigate risk of damaging persistent malware.

Pierre Louw, ESET

For endpoint security software, our research paints a mixed picture of the factors that feed into the current state of end user buying decisions. On the one hand, the cost of downtime is ranked as the single most important consideration, achieving an average score of 4.21 on a scale of one to five. This places it just ahead of upfront licencing costs, on a 4.20 average.

But other factors that make a significant contribution to a solution’s total cost of ownership are considered to be of far less importance during the procurement process, our survey indicates.

False positive rates scored an average of 3.61, while energy usage was comfortably bottom of the pile on just 2.93 out of five.

This is despite the fact that false positives – meaning wrongly issued security alerts requiring further human attention – are clearly becoming a bigger issue for many channel firms and the clients they serve.

Almost a third of our research participants said that the number of false positives issued by the security systems their organisation manages has risen in the past year. About eight per cent indicated that they have greatly increased in volume, and just 1.6 per cent had noticed a decrease.

Louw from ESET said: “False positives lead to wasted time investigating dead ends. A security analyst’s time can be expensive, and that’s time which could be spent on true positives to mitigate risk of damaging persistent malware. False positives lead to greater costs for end users and reduced security efficacy, whether they are managing cybersecurity in-house or using an MSP?”

The vast majority of MSPs taking part in our research also indicated that they face a problem from sluggish

Examining the true cost of security

performance and downtime suffered by the endpoint security systems that their organisation sells and manages.

Half of our channel chiefs said the problem was 'quite' or 'very' big, while only 8.7 per cent claimed this was 'not an issue at all'.

Vendor views

However big of a challenge is posed by these performance issues, it is clearly a problem VARs could do without.

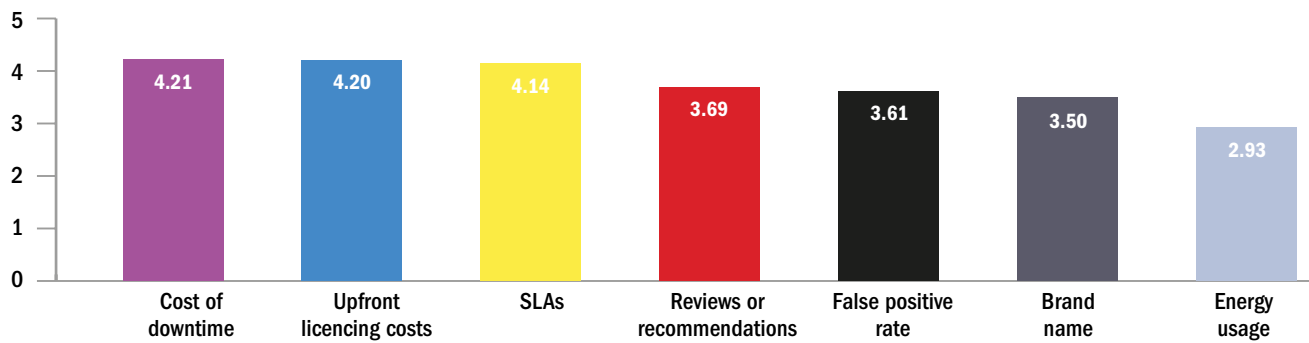
With some potentially tough months ahead, as the global economy tries to get back on its feet, the support of their vendor partners will be more important than ever.

"One thing vendors can do is help reduce the burden of

renewal management – this will free up time for channel partners to focus on new business and revenue-driving activities," Connolly said. "Increased marketing support and training can also be helpful, as well as clear guidance and, where relevant, support to help end users safely migrate systems and operations to the Cloud."

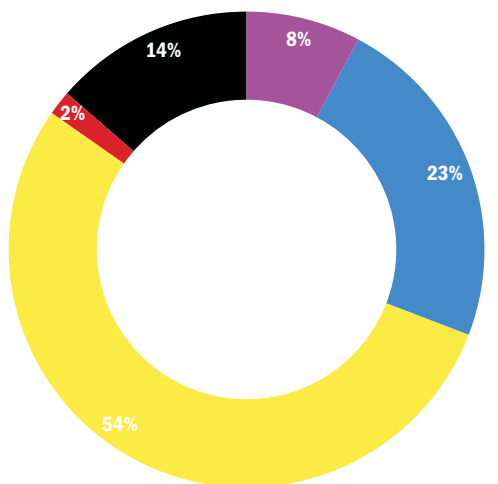
When asked to provide a little more detail on their organisation's endpoint security business and strategy, and the factors that guide it, our channel chiefs revealed that, while they like to develop long-term relationships with vendors they can trust, most are also continually on the lookout for new partners who can provide a point of differentiation.

Importance in informing buying decisions for endpoint security software*



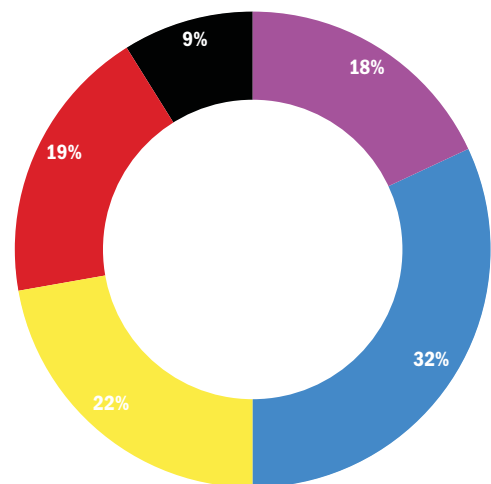
*Average on a scale of 1-5, where 1 is not at all important and 5 is very important

How have the number of false positives issued by endpoint security systems changed over the past year?



■ Greatly increased ■ Noticeably increased
■ Stayed about the same ■ Noticeably decreased
■ Do not know

How have you found sluggish performance and downtime?



■ A very big problem ■ Quite a big problem
■ Somewhat of a problem ■ A slight problem
■ Not a problem at all

Examining the true cost of security

“We have an established group of vendors, which generally continue to thrive and grow with us,” one respondent said. “A small number of established vendors do drop away, and there is also a regular addition of new, disruptive vendors.”

Another added: “We look for long-term partnerships with vendors with good reputations that offer MSP-friendly cost models. We are quite happy with the majority of our current vendors, and are currently evaluating services that address specific spear-phishing protection and cybersecurity awareness training.”

The events of the past year – and the security challenges posed by new ways of working – have only been further impetus for a “security strategy that is constantly evolving”, one channel leader told us.

“Choosing secure, cloud-based infrastructure products that offer uptime and security has been the biggest areas of focus,” they added.

In making their purchasing decisions, some customers are decidedly fixated solely on upfront costs, according to our channel chiefs, while others place a premium on buying products that are seen as a known and trusted entity.

“Initial licencing costs are a big factor for our customers and one of the key aspects they take into consideration,” said one respondent.

“Brand name and reputation are the only real considerations,” another added.

Although, on the other hand: “Most of our customers don’t care what make or brand their endpoint security comes from. They just want it to work and to not be expensive. We want both of those things too of course, but we also want it to be easily manageable – by us – and for the manufacturer to have decent support available if we need it.”

As well as these more well-established selling points, a number of our VAR leaders reported that ongoing expenses and efficiencies are becoming an ever-bigger consideration – both in regards to their existing partners and new offerings being taken on.

“We remain loyal to our long-term partners and work with them in providing information around total lifetime costs and customer success,” one said.

“We review best options for clients, in terms of licence deployment and maintenance,” according to another. “Probably a move to monthly costs from one-off CapEx has been more noticeable recently.”

“We focus on total costs from initial capital investment to recurring revenue – and not just on software costs but associated resourcing costs,” another respondent said. “Our vendor landscape has increased as solutions like containerisation have evolved and we have looked at niche players.”

It is clear from our study that resellers and MSPs are not afraid to migrate business away from manufacturer partners

who do not meet the demands of the changing world – either technically or financially.

“We have been with the same vendor for 15 or so years,” one respondent said. “Our current

provider of endpoint security has lost their way, their costs are escalating and their support is poor.”

“A recent evaluation of leading products against attacks such as ransomware clearly showed differences in effectiveness,” another added. “This has changed our product selection.”

After all, as several of our research participants pointed out, it is not the vendor’s business and reputation that is most at stake.

“Customers look to us to assess and recommend, so we need to do the homework as we don’t want to be blamed for selecting the wrong vendor,” according to one channel chief. “Our sales and marketing relies on our ability to identify the best vendors.”

“We do not sell security,” another said. “We sell ease, convenience, and peace of mind.”



Most of our customers don't care what make or brand their endpoint security comes from. They just want it to work and to not be expensive.