Clavister market survey 2022

A New Era of European Cyber Defence

Shedding light on the new cyber landscape for European Organisations

Includes results from research conducted by

COLEMAN PARKES RESEARCH

Executive Summary

Cyber security has undergone a pivotal shift in recent years. We have seen a marked increase in the prevalence of 'hybrid working' during and since the Covid-19 pandemic, which meant organisations have had to re-think their cyber security approach.

One of the biggest challenges facing organisations today is training employees how to work from home or hybrid locations securely and compliantly [i]. In fact, typical perimeter security is no longer sufficient, as the perimeter is expanding and becoming increasingly fluid as a result of hybrid working policies.

Adding to this, the Russian war on Ukraine has put businesses, especially those that comprise European critical infrastructure such as energy suppliers, on high alert as they become attractive targets for state-sponsored cyber criminals. A vast majority of security leaders anticipate a critical infrastructure breach in the coming two years [ii]. It is clear, therefore, that cyber threat awareness and contextual threat intelligence are more important than ever.

Europe can no longer afford the cyber security 'status quo'

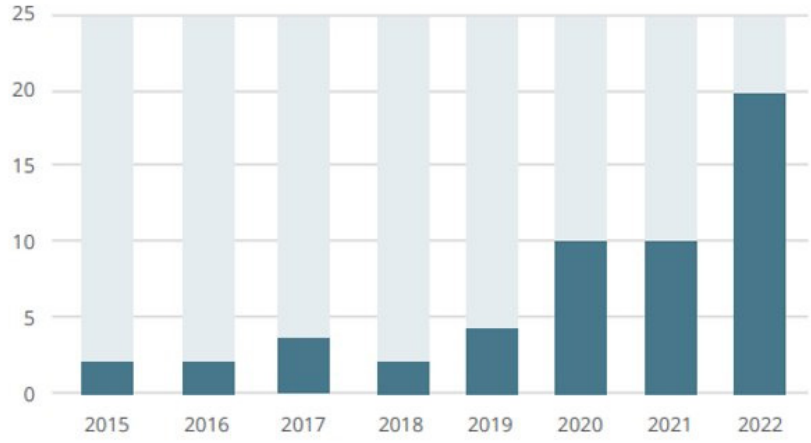
The ubiquity of cyber threats

Ransomware attacks occur worldwide every 11 seconds and cost the global economy an estimated €20 billion last year, according to Cybersecurity Ventures [iii]. Meanwhile, DDoS attacks—malicious efforts to disrupt or cut off access to internet services or websites—cost the EU economy alone roughly €65 billion in 2020.

In Belgium, for example, nearly 1,000 businesses were hit by cybercrimes in 2021—a 300% increase compared to the year prior [iv]. More than two-thirds of companies in Germany, France, Italy and the UK were reportedly targets of cyber breaches in 2021[v].

According to the UK's Cyber Security Strategy, the public sector remains a key target for a broad range of malicious actors, with 40% of incidents in 2020-21 affecting public organisations including governments themselves. The energy & utilities sector is also increasingly in the firing line since the onset of the Russian war on Ukraine.

Number of cyber-attacks on energy suppliers/year



Source: EnergiCERT

Boards are starting to sit up and take notice

However, it's not all doom and gloom. We have seen a sharp shift in attitudes towards cyber security. According to Gartner, whereas five years ago, only 58% of board members considered cyber-based threats a significant business risk; in 2021, that figure rose to 88%. This shift in perception is a welcome development.

In fact, cyber threats do not affect only our machines and work but also affect the overall society. The EU recognises that digital sovereignty is going to be one of the strategic differentiators in the coming times and that Europe needs to bolster investment to grow cyber security [vi]. We expect cyber security awareness and risk perception to spread wider in 2022, especially within Europe, given the new geo-political dynamics at play.

Policymakers and influencers are also doing their bit. The European Union is advancing legislation (through its Cyber Resilience Act [vii]) to strengthen security requirements for all digital hardware and software products. This proposed legislation mandates that products are designed, developed, and produced in ways that mitigate cybersecurity risks. The EU Parliament is also moving ahead with its NIS 2 Directive [viii], which includes a clear list of sectors and organisation sizes covered in its scope.

But what does this all mean for organisations on the ground? What and where are they planning to invest? What's important to them? Clavister conducted a market survey in September 2022 and reached out to 500 organisations, big and small, spanning energy & utilities, the public sector, retail and SMBs. This report summarises these responses and provides an insight into the current state of Europe's cyber security, its readiness to support hybrid working, and changing technology requirements since the Russian war on Ukraine.

"When it comes to cyber security, Europe is only as strong as its weakest link: be it a vulnerable Member State or an unsafe product along the supply chain"

- Thierry Breton, the EU's Commissioner for the internal market [ix]

Key Findings

Secure hybrid working has been an ongoing priority since COVID-19 pandemic and then Russian war on Ukraine aggravated the situation further

Only **1 in 3** companies think that they have good coverage to secure their remote/ hybrid workers

1/3

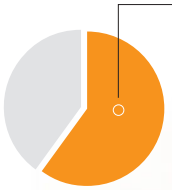
A third of organisations have made changes to their security stack/infrastructure while a further half are planning to invest in new technology!

Origin of cyber security is becoming an important consideration for European businesses. **3 out of 5** companies said they would like to see European produced cyber security!

Retail is adopting cloud fast while almost half of SMBs

44%

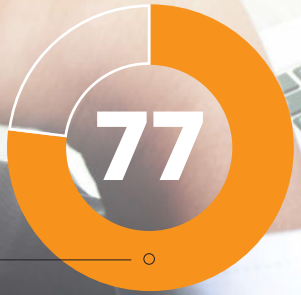
(**44%**) still prefer on-premise security!



60% of Energy & Utilities companies are willing to opt for cloud-delivered cyber security solutions

81% of Public Sector is likely to adopt 'Defence in Depth' cyber security approach

77% in Public Sector has not started or has less than **25%** of applications access using the passwordless (MFA) approach



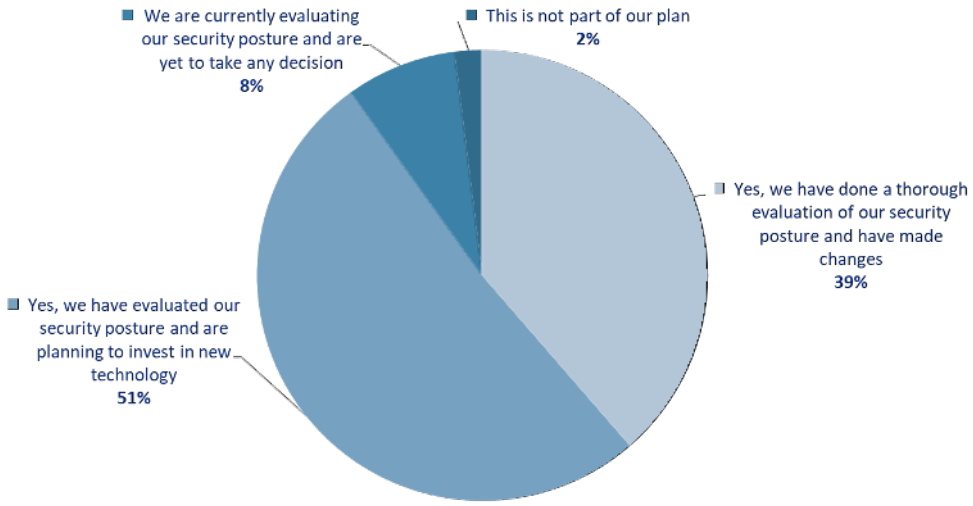
Improving security infrastructure following the war in Ukraine

We live in an era of strategic competition and complex security threats. Geopolitical shifts and the return of war in Europe, with Russia's unprovoked aggression against Ukraine, have brought cyber security issues to the forefront and forced organisations to assess their cyber readiness and make changes to their security infrastructure to improve their levels of protection.

Cyber criminals, and especially state sponsored threat actors, normally operate in hiding and attack covertly, which means that attribution has always been difficult. However, one of the shifts we have seen this year is the surfacing of certain state sponsored threat actors and groups warning businesses of the repercussions of taking sides in the Russian war [x]. This also expands their operations outside of the typical critical infrastructure and affects many more commercial industries.

Businesses and public sector organisations must reassess their cyber security strategy

The good news from our survey is that one third of respondents said that their organisations have already made changes in their cyber security stack since the start of the Russian war on Ukraine, while a further half are actively planning to invest in new technologies. This is certainly a promising start.



It's worth taking a look at where different types of organisations are on this journey.

Public sector

While the public sector has traditionally lagged behind commercial companies in terms of security coverage, it is also typically more vulnerable and has had bigger gaps to fill. Happily, the sector as a whole has realised it needs to beef up security.

92%

public sector respondents said that they have assessed their security posture and have either made changes already or are doing so currently by investing in new security technologies

Energy and utilities

Energy & utilities companies, on the other hand, seem to have started slow but are catching up fast in improving their cyber security. Convergence between IT and OT platforms and connectivity with cloud services increases the risk of a cyber breach significantly, and while IT security investments have matured, it's OT cyber security investments that energy & utilities suppliers seem to need to catch up on. From the 2021 attack on the U.S. Colonial Pipeline to a recent cyberattack on the major European oil refining hubs of Amsterdam-Rotterdam-Antwerp (ARA), there have been 48 known cyber incidents against European energy suppliers in the last five years, with 20 incidents reported in 2022 alone [xi]. Therefore, it is clear that revamping cyber security should be an urgent priority for this sector.

48 Attack agianst European energy and supply companies

31 Ransomware attacks

15 Attacks that affected OT-networks

Importance of Europe-produced cyber security

The cyber security market is an attractive market for IT professionals due to its fast-paced environment, technological innovations, real customer challenges to solve and its noble purpose of keeping society safe. It is also one of the largest users of Artificial Intelligence (AI), according to a Global AI Software Forecast 2022 by Forrester.

But for all this promise of opportunity and the range of different jobs that cybersecurity has to offer, there remain large gaps in the availability of cyber skills. Europe alone faces a huge skills gap of 350,000 [xii] security professionals in 2022. What's more, the issue is not only related to a lack of skilled professionals - Europe is also lagging behind when it comes to developing its cyber security vendor community. The US, Israel, and UK now boast well-developed cyber security clusters and cyber exports. However, how can we build trust in the European cyber security space, when most of the vendors today are from outside Europe?

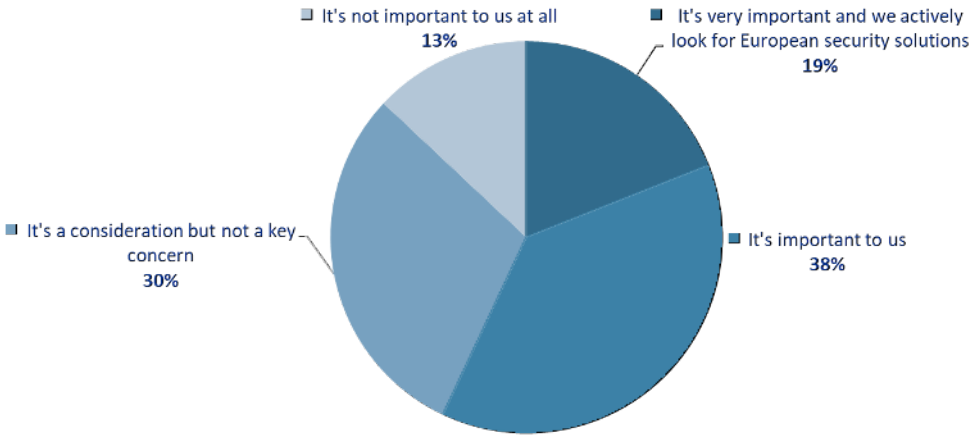
In a crowded cyber security market, who do you trust?

In the form of GDPR, the EU has implemented stringent privacy policies, but what about the question of where cyber security technology and solutions originate outside of the EU? The increased cyber threats posed by the Russian war on Ukraine have led a growing number of people to question the origin of their technology (including cyber security) in order to better understand their supply chain vulnerabilities.

The EU's new Cyber Resilience Act is also a step in the right direction, with a view to creating a single, coherent framework for compliance in the EU and to increase the transparency of cyber security practices [xiii].

European Investment Bank recently published a report that talks about the need to develop a independent European cyber security ecosystems and warns about the current investment gaps.

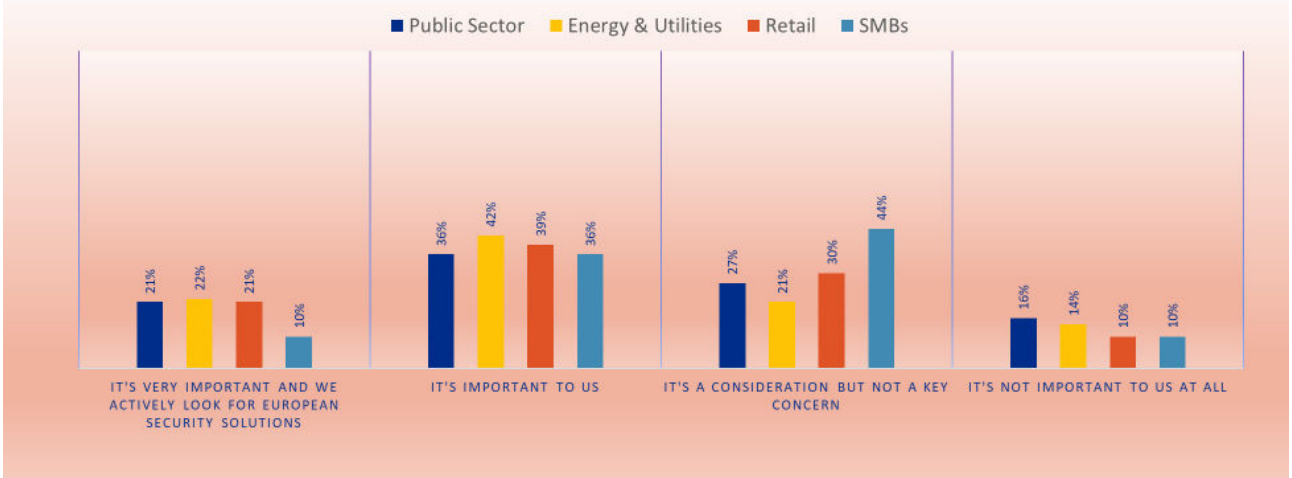
Cyber security decision makers agree with this view - more than half of them said through our survey that it is either important or very important to them that they consider European-produced cyber security products and services.



Energy & Utilities

Preference for European origin of cyber security will be greater for critical infrastructure, like energy & utilities or telecommunications.

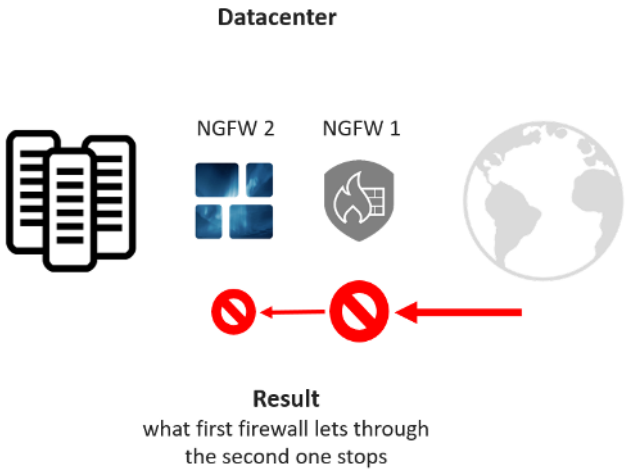
cyber security decision makers from energy & utilities sector emphasised the need for cyber security of European origin.



Defence-in-Depth for holistic protection

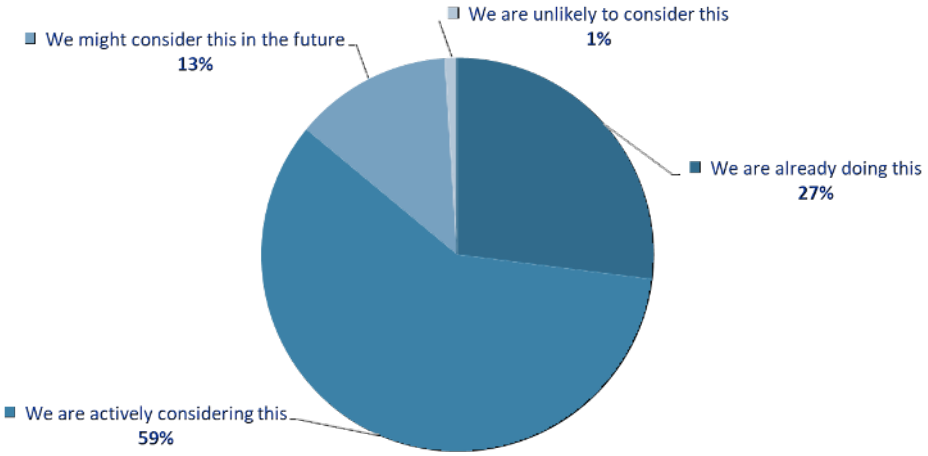
Defence-in-depth, or a layered security approach, uses multiple layers of security for more holistic protection. With this method of protection, if one line of defence is compromised, additional layers exist as a backup to ensure that threats are stopped along the way.

This concept originated in the military industry, but has since found its way into traditional perimeter-based security models designed to protect IT infrastructure. Today's cyber threats are growing rapidly in scale and sophistication. Defence-in-depth can provide a combination of advanced security tools to protect an organisation's endpoints, data, applications, and networks. A solid defence-in-depth strategy also thwarts attacks that are already underway, preventing additional damage from taking place. One example that illustrates this is the case of dual firewalls, as illustrated below:



Minimising the likelihood of a breach

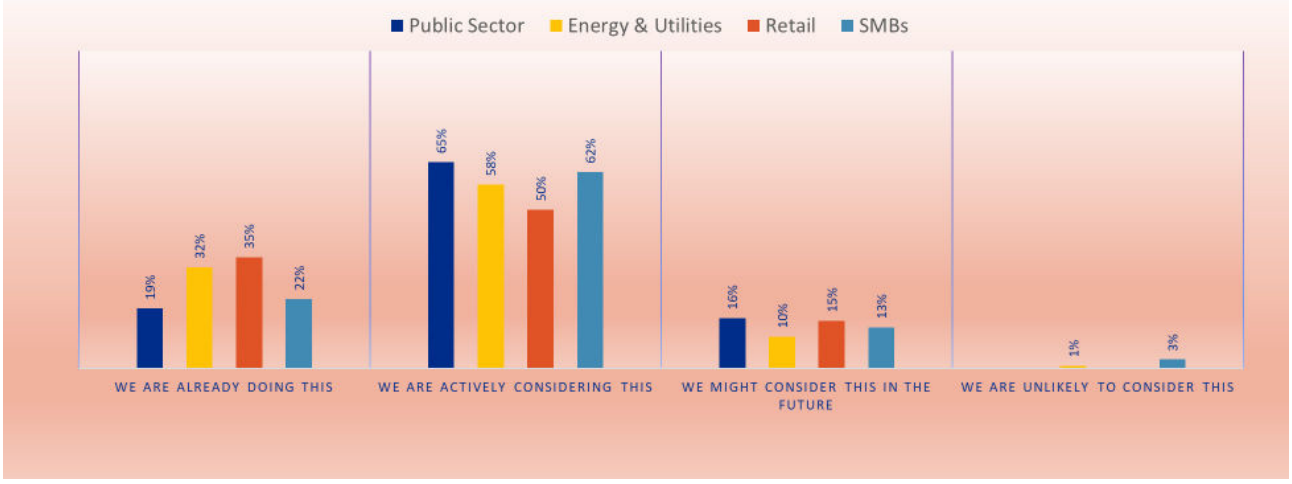
In our survey, 86% of 500 organisations responded positively when asked about layered security or 'defence in depth' approach. While 27% decision makers said that they already have multiple layers of security, an overwhelming 59% said that they are actively considering it. Another 13% said that they might consider it in future. Based on these numbers, we can safely say that awareness and preparedness seem very high and most organisations recognise that a single layer of security like a single firewall is no longer sufficient to provide comprehensive protection against today's wide-ranging cyber threats.



Retail

Awareness within the retail sector about layered defence is higher than others, partly because retail is one of the top targeted sectors due to consumer data access. And then, some of the recent cyber disruptions within the retail sector for example, 2021 attack on Coop that affected 800 branches in Sweden, impose retailers to invest actively in defence in depth and add layers to their security stack.

of security leaders in the retail sector confirmed they were using this approach already, showing a high level of maturity for layered security approach



Zero Trust using Password-less Protection

Continuing the theme of defence-in-depth, organisations today typically use a complicated network of applications including corporate data centres, private clouds, public clouds like AWS and Azure, and SaaS solutions like Office 365, Dropbox, or Salesforce.

This means that identity management and authorisation become very important, but is also extremely challenging - for example, the traditional approach requires managing multiple long lists of passwords. As a result, businesses are increasingly adopting Zero-Trust frameworks to protect against identity-based security risks.

This warrants a transition from virtual private networks (VPNs) to zero trust network access (ZTNA). Zero trust requires all users, whether inside of outside of the network, to be authenticated and authorised using a combination of preventative controls and detection mechanisms to identify attackers and stop them from reaching their goals once they do penetrate a network. Foundational components of Zero Trust including SSO, MFA, Device Trust and, more recently, 'passwordless'.

'Passwordless', as the term suggests, involves describes systems that eliminate the need for passwords entirely, whereby users identify themselves via an authentication token assigned to the user and device, in turn preventing access from unauthorised devices and credential theft. Rather than deploying time-consuming and expensive ways to manage passwords that overwhelm IT teams, passwordless authentication maintains authentication flow while retaining MFA security. It enhances security while also decreasing authentication friction for users, meaning IT teams can benefit from 'the best of both worlds'.

Promisingly, we found that almost 70% organisations have either started to implement 'passwordless' login for corporate applications or it is in active consideration.

Passwordless - The next step in the Zero Trust journey

However, of those who had already started this process, most had done so only to a limited extent. When we asked what percentage of online applications available to employees are available as 'passwordless' login, majority of them replied between 1-25%.

Larger enterprises have a far more complex environment that requires more work to integrate with passwordless technology however the gain in security levels is also greater for them.

of SMBs have started to use 'passwordless' login for 26-50% of applications, often covered by Microsoft 365 or Google Suite program.

Growing Interest in Cloud-Delivered Cyber Security Deployment Models

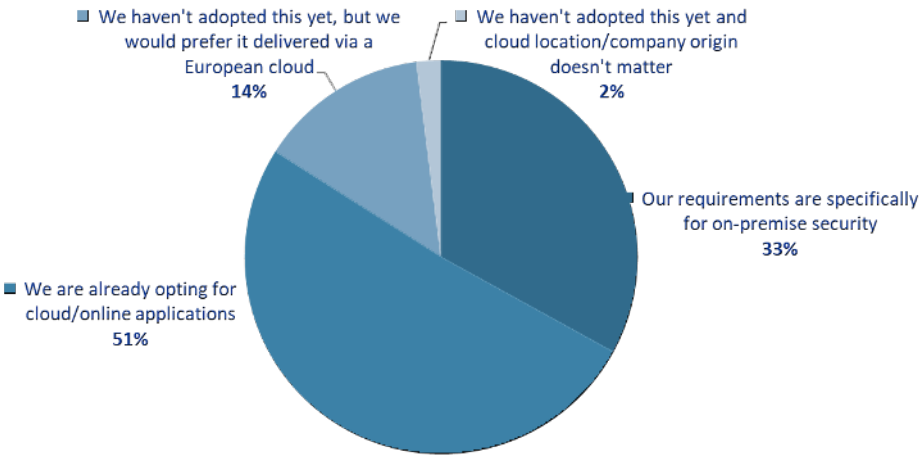
While on one end of cyber security spectrum, we have on-premise security, the other end includes cloud-delivered security or security as-a-service. On-premise security has been the most dominant mode of deployment so far, however the more enterprises move toward cloud, cyber security requirements also move into that direction.

Cloud-delivered security can be easier to implement and maintain, since the security technology is updated and maintained by an external provider. It is also a less expensive way to acquire newer security solutions because

Broad adoption of cloud-delivered cyber security

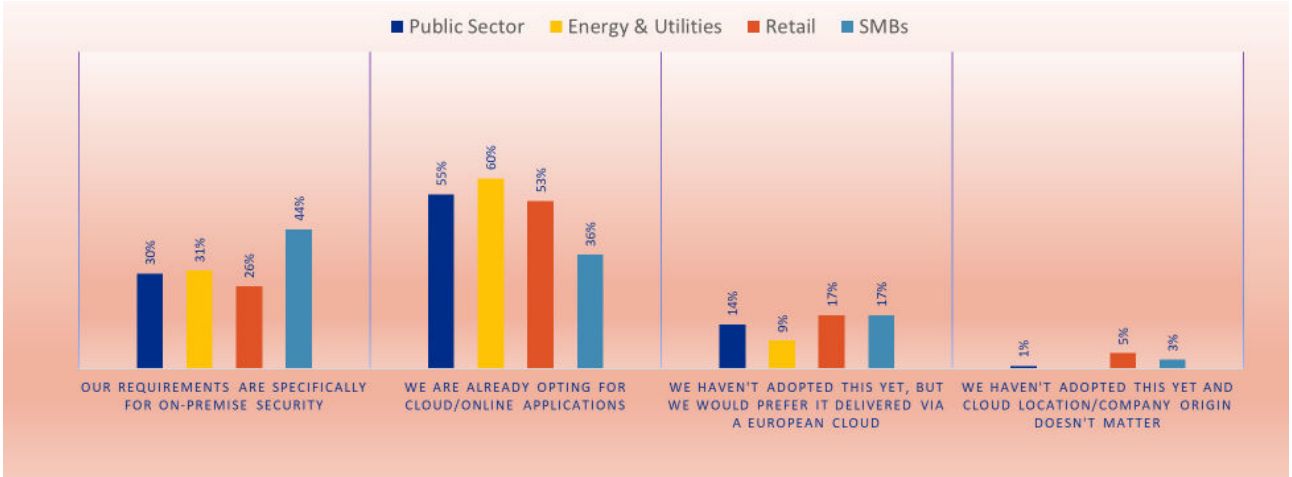
cloud-delivered security is usually based on a subscription model, therefore less capital expenditure. Cloud-delivered security also provides the benefit of scaling as per demand due to elasticity of cloud environments.

When we asked cyber security decision makers about their preference when it comes to cyber security delivered as a cloud/online application, half of them responded saying that they are already opting for a cloud-based approach.



The public sector and energy & utilities sectors are leading this adoption, no doubt influenced by the fact that these sectors have increased their cyber security spending in the recent years (as evident in our initial survey responses) and are therefore opting for more recent modes of deployment of security.

Nonetheless, on-premise security products are here to stay, at least for the time being. Overall, one-third of organisations said that their preference is still on-premise, and this preference is even higher for SMB organisations.



A possible explanation for these numbers could be that SMBs have historically invested in more traditional security products like firewalls, which have been slow to move across to cloud delivery. Identity and Access Management (IAM) and email security are among the more commonly solutions delivered via the cloud and adoption of these solutions has typically also been slow among SMBs.

While cloud-delivered security certainly has advantages compared to on-premise security, one important limiting factor could be the privacy of the technology being delivered. This is because a third-party typically manages the system, leading to possible data residency and compliance issues.

One potential solution to this challenge is cyber security delivered via a European cloud.

In our survey, 17% among the retail sector and SMBs decision makers said that they would prefer their products and solutions delivered via a European cloud.

This is a surprisingly high figure considering not many vendors in Europe are currently offering this service but there clearly is an appetite for it.

Maturity of security infrastructure to support hybrid working

When the Covid-19 pandemic and lockdowns forced employees to work from home, one of most employers' urgent requirements was to make sure that employees have the necessary infrastructure and access to corporate networks to be able to work from home.

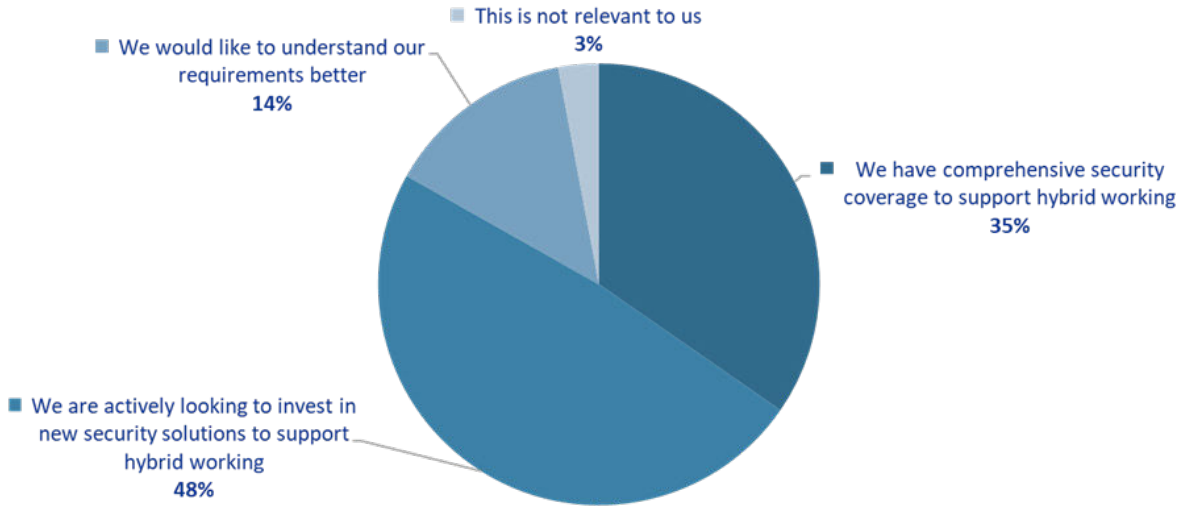
However, as that time has now mostly passed and we have firmly moved towards hybrid working, employers are having to re-think cyber security properly and ask questions about where the organisation's data resides, who has access to it and how it is protected and accessed. Focus has largely shifted to ensuring a safe and secure working environment, expanding cyber security coverage to wherever the worker goes.

In previous sections, we touched upon transition to Zero Trust and a shift towards cloud-delivered cyber security. Combine this with hybrid working and interestingly enough, these are the exact three trends that are influencing growth in the cyber security market, according to a recent report from Gartner [xiv]. In that context, our survey report provides concrete data further validating these trends from a European perspective.

In our survey, only around a third of companies felt they already had comprehensive security coverage to support hybrid working, but the encouraging response is that almost everyone understands its importance and that they need to take action now.

Organisations are not yet confident in their abilities to support hybrid working

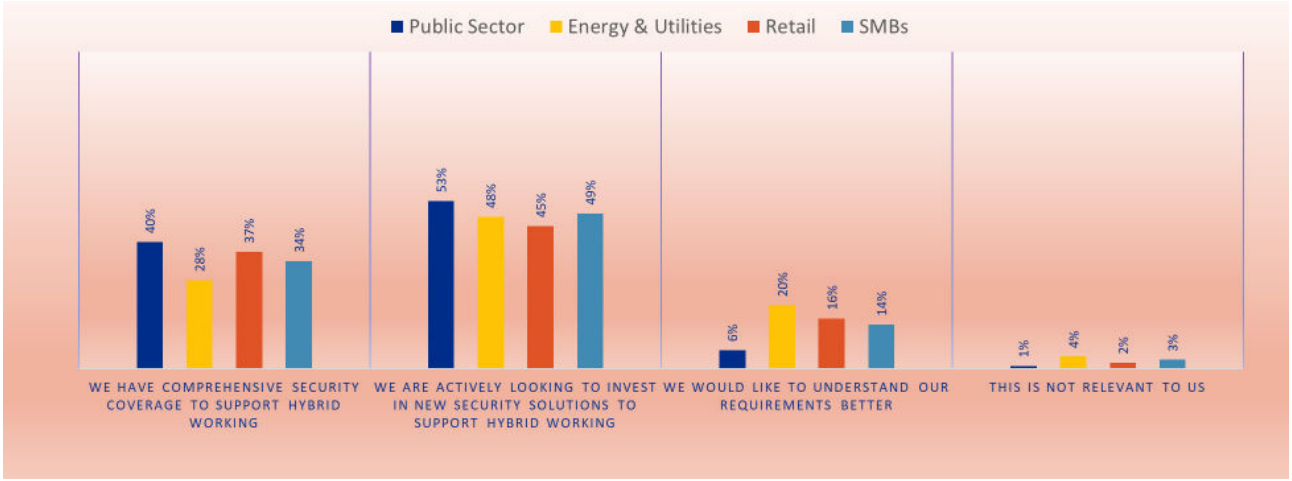
Three factors influencing growth in security spending are the increase in remote and hybrid work, the transition from virtual private networks (VPNs) to zero trust network access (ZTNA) and the shift to cloud-based delivery models, according to Gartner, Inc.



When the COVID pandemic struck, public sector was possibly the least prepared sector to move to work from home or hybrid working. Therefore, they had to make the most arrangements and largest investment into cyber security.

Energy & utilities industry on the other hand side, has been slower on the uptake but willing nonetheless and if they are not already on the investment spree then they are spending time in understanding their security requirements better.

However, its good to see that public sector is leading the preparations, with 51% actively looking to invest into new technology to secure hybrid working.



In the End...

It is clear that European organisations face a new landscape of cyber security today – from the technological changes taking place to adapt to hybrid working policies to the complex geopolitical dynamics associated with the Russian war on Ukraine. Promisingly, our research has shown that businesses and decision makers across the board are beginning to take seriously the changing requirements of this new era.

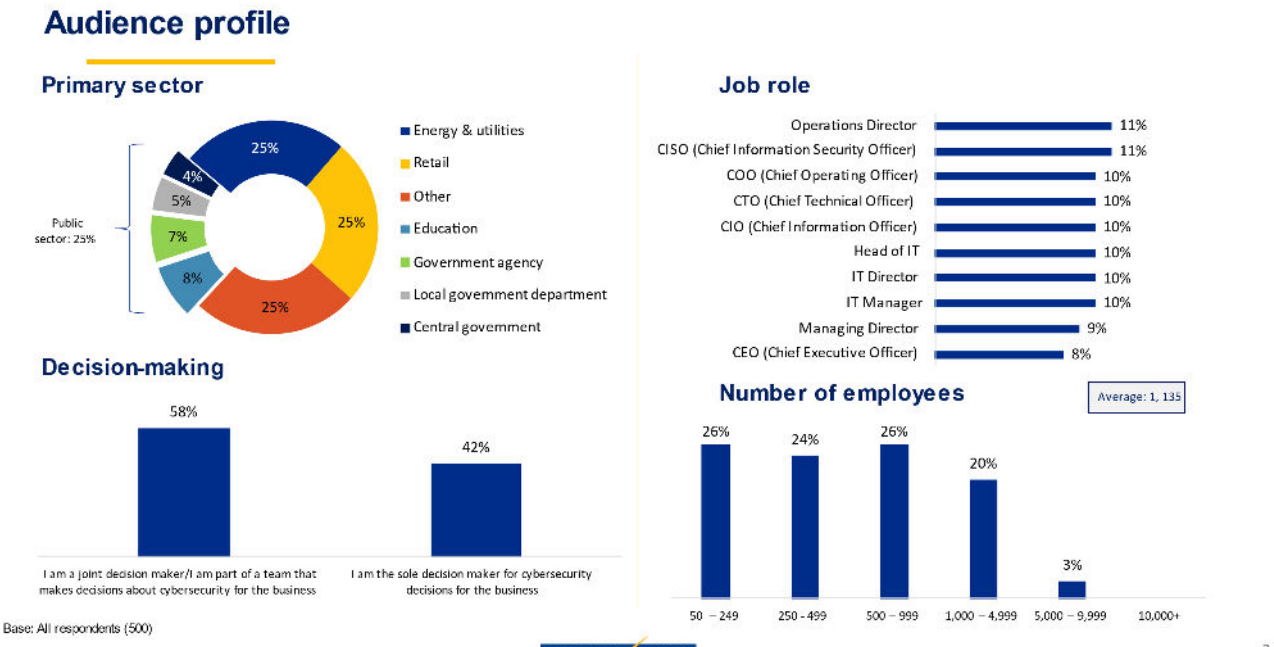
At board-level, companies are increasingly taking notice that change is needed – in many cases, they are already acting upon this trend.

Whether this be on the importance of cyber security products and services originating in Europe or taking heed of the advantages of Zero Trust and cloud-based security, we are seeing positive steps in the right direction.

European organisation can no longer afford to maintain the cyber security 'status quo' and are actively looking to increase investment in improving their coverage across the board – from the public sector to retail and energy & utilities, businesses must continue prioritising holistic protection to address the myriads threats they face.

About this Market Survey

This survey was conducted by Coleman Parkes Research in September-October 2022 and targeted 500 cybersecurity decision-makers in Sweden in organisations with more than 50 employees, focusing on SMBs and the public, energy & utilities and retail sectors.



About Coleman Parkes Research

Coleman Parkes Research is a full-service B2B market research agency specialising in IT/technology studies, targeting senior decision makers in SMB to large and enterprises across multiple sectors globally.

For more information, contact research@coleman-parkes.co.uk

About Clavister

Clavister is a specialised European cybersecurity company, protecting complex digital businesses for over 25 years. Founded and headquartered in Örnsköldsvik, Sweden, Clavister pioneered one of the first firewalls and continues to build robust and adaptive cybersecurity solutions since. Empowering a growing ecosystem of partners and resellers, we have been serving customers in more than 100 countries with 125,000+ deployments across public sector, service providers and defence sectors. Network, cloud, mobile, end points – we secure them all.

For more information visit www.clavister.com

About "CyberSecurity Made In Europe"

The Cybersecurity Made In Europe Label is issued by European Cyber Security Organisation (ECSO). ECSO is a European, cross-sectoral membership organisation that contributes to developing cybersecurity communities and building the European cybersecurity ecosystem. Clavister is a proud member of ECSO, helping to enhance European cyber security.

For more information, visit https://www.cybersecurity-label.eu

CYBERSECURITY™
MADE IN EUROPE

Appendix - references

i https://www.forbes.com/sites/forbestechcouncil/2022/11/01/top-three-challenges-facing-cios-in-2023/?sh=41d31b9c7f90

ii https://www.pwc.co.uk/press-room/press-releases/two-thirds-of-uk-business-leaders-expect-cyber-security-threat-t.html

iii https://cybersecurityventures.com/cybercrime-infographic/

iv https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2022/january/mastercard-reveals-record-levels-of-cybercrime-in-belgium-during-the-pandemic/

v https://www.dbxuk.com/statistics/data-breach-statistics

vi https://www.bankinfosecurity.com/europe-looks-to-boost-domestic-cybersecurity-investment-a-20307

vii https://www.european-cyber-resilience-act.com

viii https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

ix https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/

x https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

xi https://insightevents.dk/isc-cph/2022/10/06/protecting-our-critical-infrastructure-has-never-been-more-important/

xii https://www.orange.com/en/newsroom/news/2022/cybersecurity/why-does-european-cybersecurity-pose-talent-challenge

xiii https://datainnovation.org/2022/09/an-overview-of-the-eus-cyber-resilience-act/

xiv https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i

SECURITY BY SWEDEN

clavister®

CONNECT • PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 • **Web:** www.clavister.com