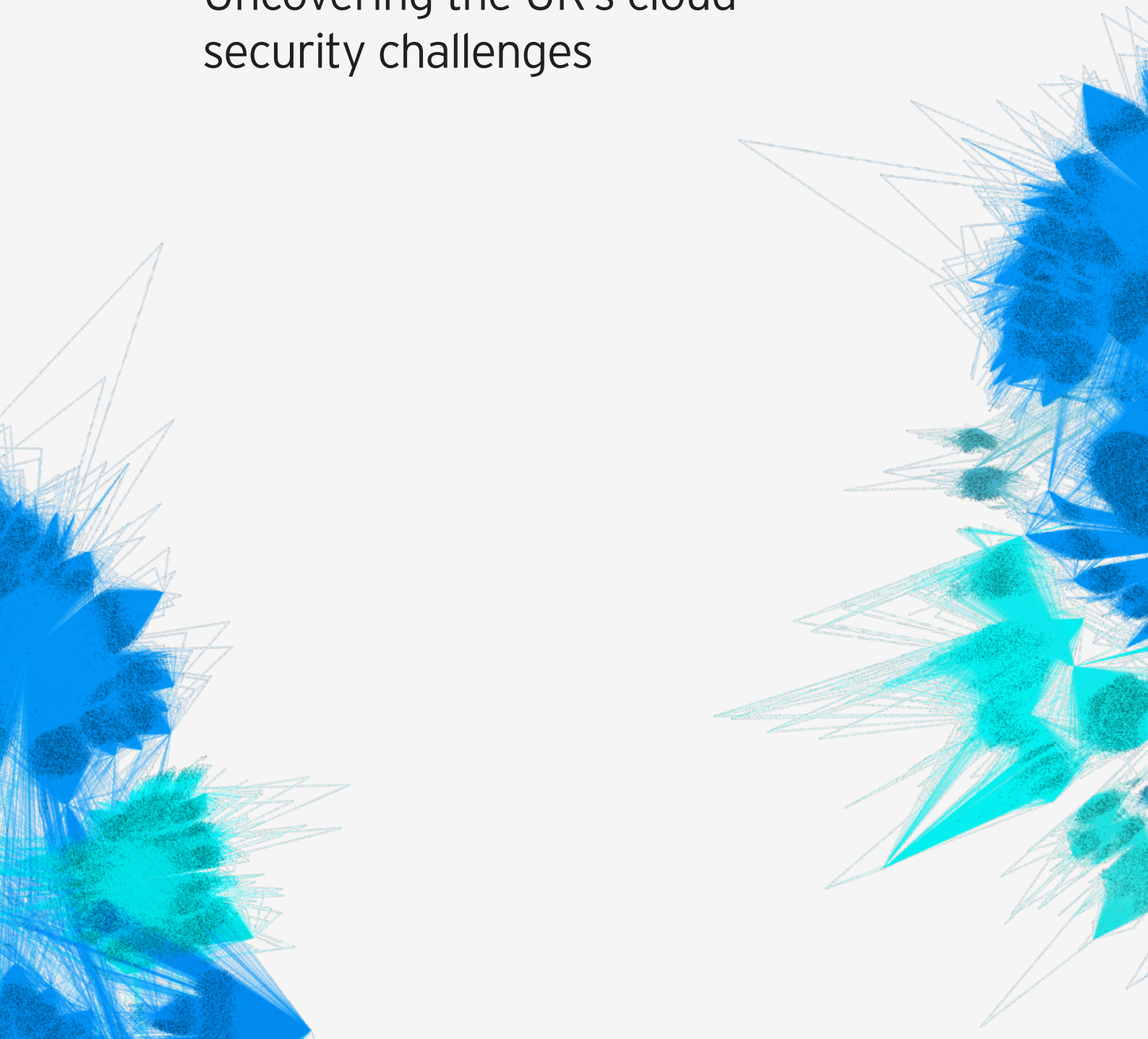
Perception and reality:

Uncovering the UK's cloud security challenges



Riding the crest of a digital wave

COVID-19 has been responsible for arguably the biggest acceleration in digital transformation ever seen. Back in May 2020, McKinsey claimed that consumer and business adoption of technologies like cloud computing had "vaulted five years forward" in the space of just eight weeks. This is great news for the cloud providers themselves, of course. But more importantly it has helped organisations to redesign business models, support mass remote working, and reach out to their customers in spite of nationwide lockdowns and social distancing mandates.

81%

81% feel their cloud adoption plans have accelerated

However, when organisations expand their digital footprint, it can also lead to unexpected outcomes: cyber-criminals are past masters at exploiting security gaps to further their own ends.

We wanted to understand more. How fast and how far are UK organisations actually digitally transforming during this period of unprecedented change? Where do they believe their biggest security challenges lie? And how confident are they in facing these threats going forward?

To find out, Trend Micro commissioned Sapio Research to poll 100 IT decision makers in the UK, as part of a wider global report covering 28 countries. Respondents came from a wide variety of verticals and ranged from IT managers up to the C-level in SMBs with 250+ employees all the way up to large enterprises with 10,000+ staff.

As we'll discover, UK IT leaders are extremely confident in their ability to protect their organisation from surging cloud threats. The issue is that in many cases there is a disconnect between this stated confidence and the admission that security continues to be a major barrier to adoption of cloud technologies. Some responses also highlighted a misunderstanding of key cloud security concepts and the capabilities of modern solutions.

Like their global counterparts, UK IT leaders are in no doubt that COVID-19 has accelerated their cloud adoption plans. Some 81% claimed it had "considerably" or "somewhat" hastened technology investments in this space. Whether it's a simple purchase of video conferencing software or larger scale infrastructure spending to support innovative new customer-facing applications, there's no question of the value of cloud amidst the pandemic.

Respondents are also keeping one eye on the future—investing in cloud to ensure their organisation is in a strong position when it exits the pandemic. To maximise their capabilities, a third (34%) said they'll be developing cloud native apps, while nearly half (48%) will be mainly "lifting and shifting".

Confident about cloud security

As part of these efforts, UK IT bosses are ensuring they pay attention to cybersecurity. Over half (56%) said they already have, or plan to implement security training and 47% said the same about audit procedures and guidelines.

Despite the potential for new threats, most (52%) said they believe cloud adoption has actually increased their focus on security, while a third (33%) said things were unchanged. The vast majority (92%) felt totally (24%) or mostly (68%) in control of securing the remote working environment. And a mean of 72% were confident in their visibility of corporate data, even as it flows across distributed cloud environments.

56%
have a plan in place for security training

52%
have an increased focus on security

72%
are confident in their visibility of data

This confidence comes amidst a surge in digital threats capitalising on the pandemic. These include:

- Ransomware, which is a growing risk for larger organisations, as threat actors look to take advantage of distracted IT teams and employees. In many cases, sophisticated groups are using tools, tactics and procedures similar to APT actors—such as long periods of reconnaissance prior to compromise and the use of legitimate Windows tools to stay hidden while moving laterally within victim networks.
- Targeting of remote workers with COVID-themed phishing lures. Trend Micro alone observed nearly nine million such threats in the first half of 2020. Sometimes employees are their own worst enemy, disregarding best practice training to engage in risky behaviour such as uploading corporate data to non-work apps.
- Attacks exploiting human error in cloud configurations, which could leave sensitive data stores exposed to the public-facing internet. Trend Micro identifies on average 230 million such mistakes every single day for its customers.
- The exploitation of known vulnerabilities and use of previously breached passwords or easy-to-guess/crack credentials has also been on the rise as cyber-criminals look to compromise cloud accounts and systems to monetise attacks.

Despite these risks, most (58%) respondents claimed that their current security budget fully matches their organisation's cloud ambitions. An overwhelming 90% said they felt fully or mostly in control of securing the hybrid working environment set to become the norm in a post-COVID world.

The reality of cloud threats

However, here's where we began to detect some inconsistencies in respondents' attitudes to cloud security. Despite their headline confidence in being able to handle most cyber-threats, two-fifths (40%) admitted that security was a "very significant" or "significant" barrier to cloud adoption—rising to 63% when including those who claimed it would be a "moderate barrier". It's a pattern repeated globally, and would seem to indicate that there are indeed challenges for many IT leaders in this space.

In fact, UK respondents claimed that their biggest day-to-day headaches in securing cloud workloads were patching (43%), setting consistent policies (32%) and deployment (31%). As we shall discuss, with the right automated tooling, these need not be major challenges for IT teams.

Also concerning is that, as elsewhere around the world, IT leaders in the UK seemed unsure of the meaning of Shared Responsibility, the model which governs how much of the cloud stack customers must secure, versus providers. It is widely understood that customer organisations are responsible for protecting all data and applications in their IaaS and PaaS environments and all data in their SaaS environments.

However, respondents claimed that their cloud provider offers either "more than enough" (45%) or "sufficient" (55%) data protection capabilities. This is despite the vast majority (93%) stating they were confident they understood the Shared Responsibility model.

Day-to-day security headaches include:

- 43% Patching
- 32% Setting consistent policies
- 31% Deployment

Barriers to deploying cloud security include:

- 40% Worries about privacy
- 37% Budget
- 35% Training

A more secure future

Further responses also seemed to indicate a certain amount of misunderstanding about the cloud security market and how best to manage cyber risk. Over a third of UK IT leaders claimed that the introduction of cloud security tools had made the job of their IT security teams more difficult (35%) and more costly (34%). Just 21% said it had made work less difficult and just 15% that it had reduced costs. Many also claimed that privacy (40%), budget (37%) and training (35%) issues present barriers to migrating to cloud-based security tools.

In fact, SaaS-based cybersecurity should be cheaper, quicker and easier to deploy for IT teams, and help to save on upfront CapEx costs. The right tools should not present any kind of privacy risks and require little training to get up-and-running. Modern security platforms which offer automation and support for both on-premises and hybrid cloud environments can deliver powerful protection capabilities from a single-pane-of-glass user interface. In so doing, they're able to reduce many of the operational challenges listed above via virtual patching, automated deployment and seamless policy management.

UK IT leaders pointed to network-layer protection, Cloud Security Posture Management (CSPM) and Cloud Access Security Broker (CASB) tech as most important in helping them protect their growing cloud environments. These are certainly important components. But arguably more important still is finding the right security partner to support a multi-layered cloud security strategy that leaves no gaps exposed.

As organisations look to digitally powered growth to propel them out of the pandemic, they must focus first on building a secure foundation.

TREND MICRO™