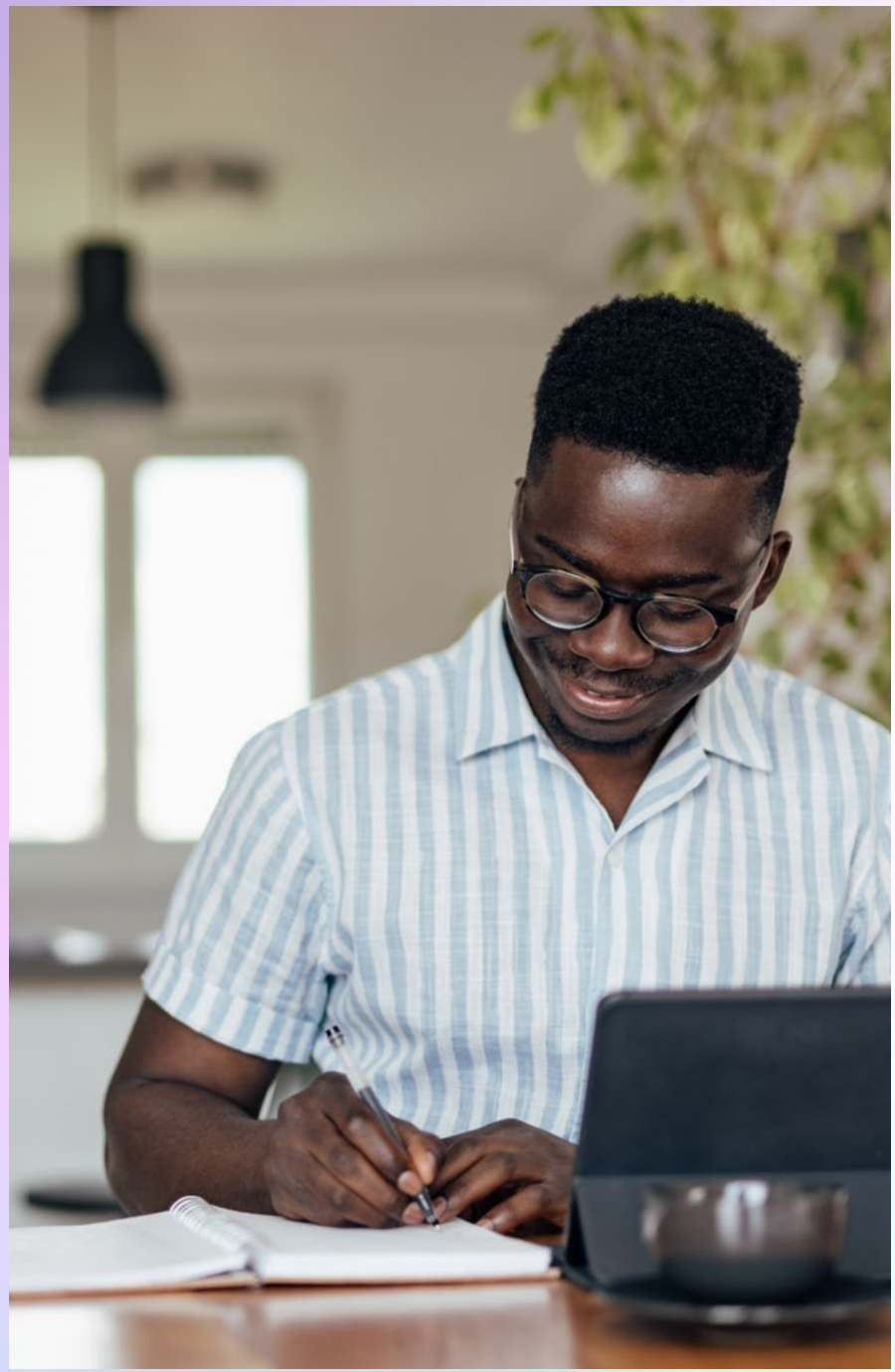
BT Means Business

The future of work is already here.

Now's the time to secure it

Robust security to protect and enable your business

Kevin Brown
Managing director, BT Security



Introduction

These are exciting times. Businesses everywhere are looking ahead at new ways of working, innovating with the latest technology, and undergoing impressive digital transformation.

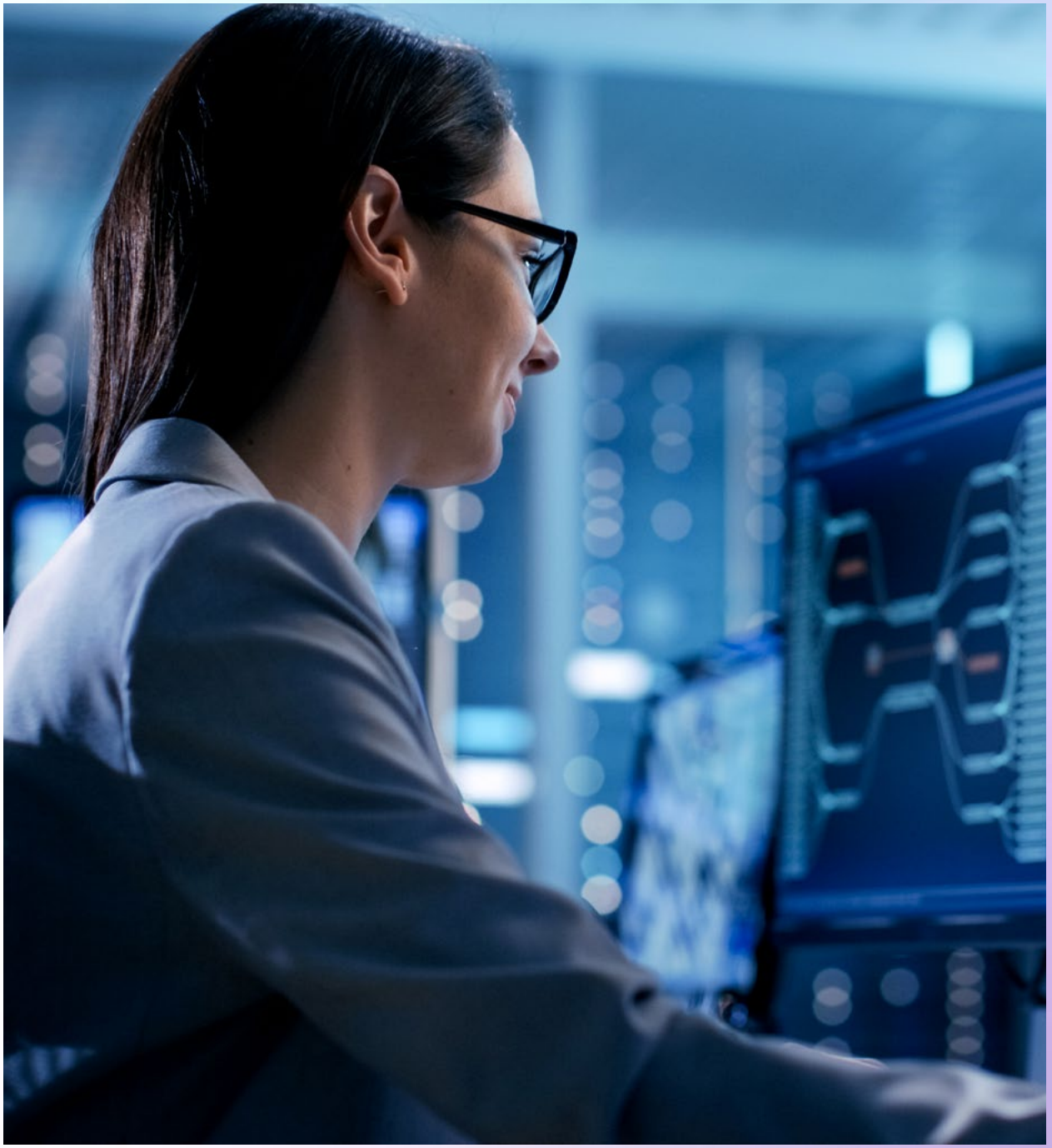
Multiple operations are moving to the cloud and in this post-pandemic era, working remotely is no longer a perk, it's an expectation. Meanwhile, shiny new tech abounds and intriguing inventions from the 'Internet of Things' are adopted at scale. The future of work has arrived and triggered a revolution.

And yet lagging behind all this innovation are the cyber-security measures it depends on to support it. Every 19 seconds, an organisation is hacked in the UK.[1] According to **Gov.UK**, 72% of larger firms identified a cyber-breach or attack from either individuals or state sponsored operations. The current landscape of changing work practices, cyber-skill shortages, and geopolitical tension is creating a perfect storm for attackers. Cyber-criminals are increasingly sophisticated and funded – and businesses are grappling with complicated regulation and policy.

1 National Cyber Security Centre

You already know that cyber-security is critical for the protection of your business. But, more than that, it's how you'll ensure the success of the future of work within your organisation. It's how you'll build a secure foundation to innovate from, that enables your people to be flexible about where and how they work. And it's how you'll grow the organisation in confidence – unencumbered by avoidable financial and reputational damage.

We'll be exploring the importance of elevating the status of security within your business to achieve strong, simplified, and consolidated protection against the growing threats. Not only to protect your people, your workplaces, and your business, but to boost your resilience so that you can innovate freely – from a safe place – and maximise the positive impact that new technology can bring.



Knowing what to protect

Almost all organisations are now questioning how secure they really are, and whether their defences are actually protecting them. What might have once seemed like a level of paranoia reserved solely for the CISO has now become the norm across all organisations.

Cyber-security effectiveness comes from being proactive and staying ahead – rather than chasing a horse that's bolted. Understanding the full picture and knowing where the vulnerabilities lie is essential.

Cyber-attacks and data breaches can happen to any business at any time – they don't come with a friendly warning and the impact is not insignificant. Imagine what the cost to your business would be if it was unable to operate due to a cyber-attack. One report found that the average downtime after a ransomware attack is 21 days. Attacks are also on the rise with phishing scams being the most common at 83% of UK businesses surveyed in 2022.[2]

Cyber-crime is an ever-present and ongoing threat. For context, at BT, we block 6,500 potential attacks a day and over 100 million malicious communications every month. Fortunately, we have a robust cyber-security infrastructure to remove access points for these attackers. But these numbers are staggering and the gaps, if left wide open, will undo all the efforts and investment spent. Here are five major areas within cyber-security that organisations are under pressure to get right:

2 **Cyber Security Breaches 2022**

1. Increased volume of data and threat

In years gone by the problem was a lack of data to make insightful decisions – but we're now facing the 'data paradigm', where this situation has completely inverted. There's now far too much data to ingest, and many organisations are struggling just to keep up, often using operating models that were devised several years ago which don't take the multi-cloud era into account.

BT's cyber-security platform processed 100,000 cyber-events a second in 2018 and today it's over two million per second. In total, that's 170 billion events which we ingest and analyse every day to defend our network against cyber-attacks around the clock. Many organisations are innovating just to keep their heads above water – but this isn't sustainable. We need to challenge how we see innovation – not using it to adapt and react, but to create a fundamental step change in our outlook and approach.

2. Flexible working and a shift to the cloud

The workplace has evolved to offer employees alternate ways of working. We've seen a 62% increase in daily traffic on our network since the first lockdown. UK broadband usage more than doubled in 2020, driven by live sport, online gaming, and homeworking.[3] These are strong signs that so much of our life has migrated online. And it continues to do so – in the past three minutes, hundreds of terabytes of data will have gone across BT's network.

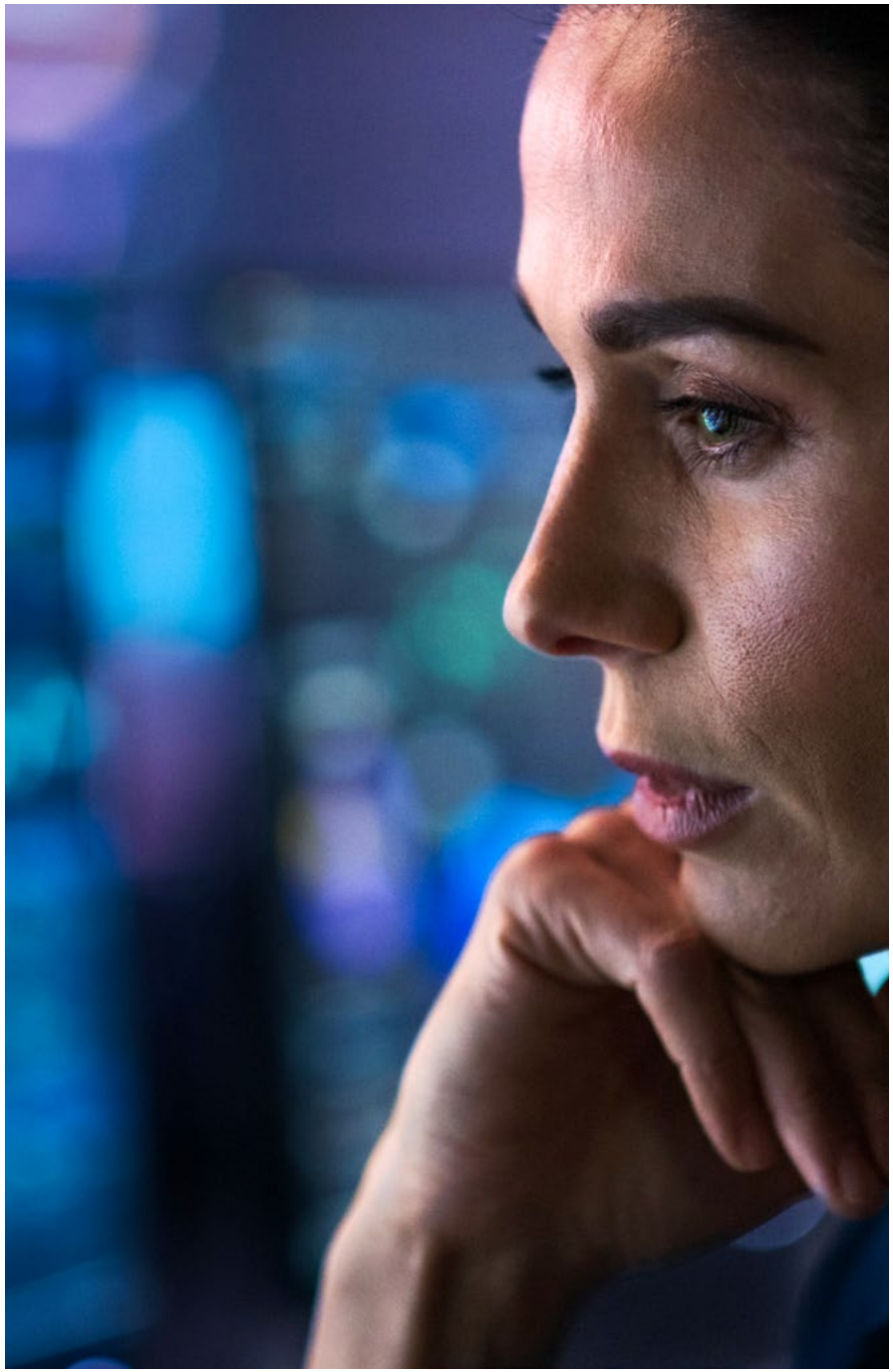
While this is positive for the employee looking for flexibility, it's leaving vulnerable gaps in the security system. For example, 69% of companies have suffered a cyber-security incident as a direct result of teams working remotely. And while two thirds of UK business leaders expect a jump in attacks on their cloud services over the next year, only 41% say they understand the risks.[4]

3 **Openreach**
4 PwC

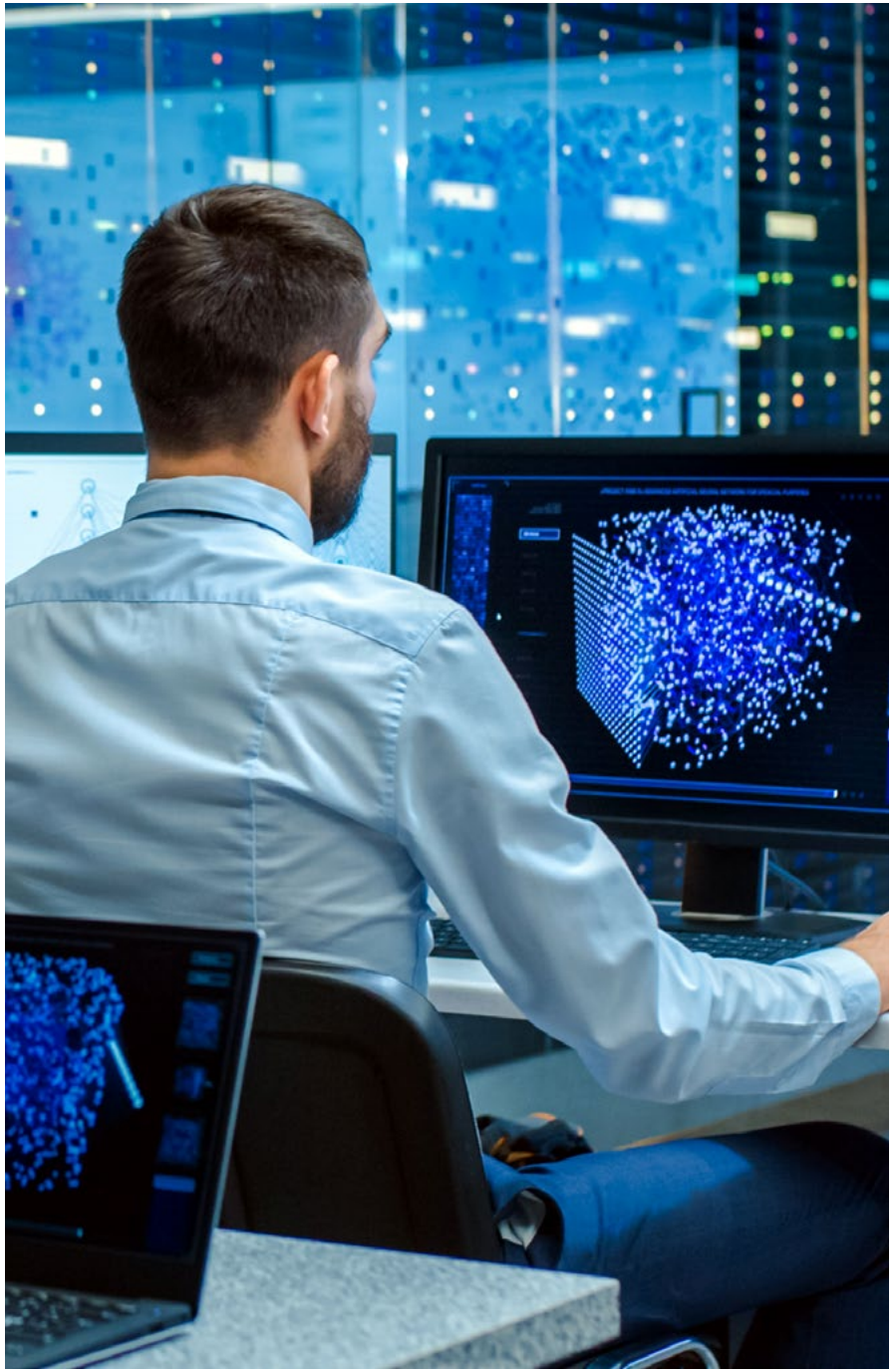
3. Disjointed security measures

The connected nature of technology today has massively increased even in the past two to three years – now allowing attacks to spread much more quickly. Fragmented security solutions have been retrofitted to new ways of working leaving patchy protection in their wake. This has been exacerbated by events such as the pandemic when businesses had to get their teams up and running remotely overnight.

According to Mandiant in 2020, 53% of malicious attacks were missed by existing tools.[5] Security from multiple providers give companies less visibility of what's being protected and by who. And this really matters, as you're only as secure as the weakest link in your chain. Security organisations and cyber-criminals are now in a constant race to identify these weak links. It's no longer just about protecting yourself or one type of industry in isolation. Today's cyber-landscape is all about interdependencies.



5 Deep Dive into Cyber Reality, Mandiant, 2020



4. Cyber-skills gap

Businesses, globally, are experiencing a cyber-security skills shortage. And with a lack of internal resources (with the right knowledge) they're missing the threats. Only 41% of organisations say their IT security team is effective in determining and closing the gaps in their IT security infrastructure.[6]

The irony is that while recruiting and training takes time and investment, almost 40% of organisations are wasting their cyber-security budgets because of skills shortages.[7]

5. Staying locally and internationally compliant

In today's global marketplace, understanding and dealing with complex security compliance and regulatory requirements is a challenge. Organisations face legal, financial, and reputational risk if they fail to comply. But with such a complex landscape of laws, knowing you have it all covered isn't always straight-forward.

6 **Security Bitesize, Security Advisory Services, October 2020**
7 Teiss

Prioritising three core areas

We know that the future of work depends on having the resilience and stability to navigate digital transformation without being left wide open to cyber-attacks.

But, for large organisations, there's a lot to consider – your entire infrastructure, to be precise. It can be overwhelming when considering how to protect the business, so instead let's break it down into three strategic areas.

These are your people, workplaces, and your overall business. All three need to be aligned in their protection to provide a safe space and working culture that delivers the best employee experience. And if just one isn't done right, it will leave the gaps open and impact the strength of the others. Here's a breakdown to this three-fold approach and how you can make each as robust as they need to be.

1. People at the heart

Businesses need to drive secure productivity, collaboration, and access to services wherever employees are located. You need your people to be able to collaborate, sell, and operate securely – without compromising on efficiency or employee experience. Enabling your employees to work in a way that suits them is key to fostering a good employee experience and reducing attrition.

As your employees are working from anywhere and on all devices, they need protection that measures up. Your business simply can't afford to risk losing 21 days of productivity due to ransomware, or the impact on your reputation. At the same time, you need employees to be able to focus on their job, without distraction, reassured that their security is being taken care of.

This means 24/7 real-time monitoring and full visibility of who and what is connected to the network at all times for proactive threat detection and mediation. It means implementing a single policy and configuration management across multiple users and devices to reduce cost and time. And it needs to be a solution that can scale as your workforce grows.

2. The safest workplaces

It can't be said enough: all workplaces (whether digital or physical) must be secure at all times. But with so many people working in varied places with a hybrid or fully remote set-up, it's a challenge. Businesses need 24/7 protection that can scale when new sites arise, along with dynamic policies that can flex around a borderless estate.

Transformation relies on making offices, sites, and remote working more efficient and securely connected. You need users of cloud-based tools and applications to be secure and compliant while having flexibility to respond to changing hybrid work patterns. But you're facing threats from data stored in multiple locations – and your business, like 72% of organisations, may be struggling to source the cyber-security talent to enable this.[8]

Then there's the hybrid cloud migration which, if insecure, can lead to data loss, lack of visibility and security breaches. So, you'll need a solution that seamlessly integrates with your existing cloud set-up, plus end-to-end protection of your network across multiple locations. Put simply, to future-proof your investment and maximise potential, your security solution must be able to outsmart attackers from absolutely every angle.

8 Cyber Security in Focus Survey 2020, Stott and May

3. A business with confidence to thrive

Cyber-risk is considered by 74% of executives as one of the top-three threats their company faces today, while only 36% strongly agree that their current processes enable them to securely achieve their business objectives. If you think your organisation is in the same boat, it's time to start thinking holistically.

Zoom out for a moment and look at the bigger picture – your business as a whole. Because this is about future-proofing your security strategy, not retro-fitting cyber-tactics. Developing a roadmap for the next five years is a crucial step towards gaining a strategic advantage in the future of work.

To compile this road map, you'll need a solid understanding of your security posture – not just today, but every day. And to manage this, the help of an expert who can keep monitoring and testing your defences so you can respond in real time is recommended. After all, your approach to cyber-security deserves to be underpinned by the best thought leadership and smartest technology.

Safeguarding from end-to-end

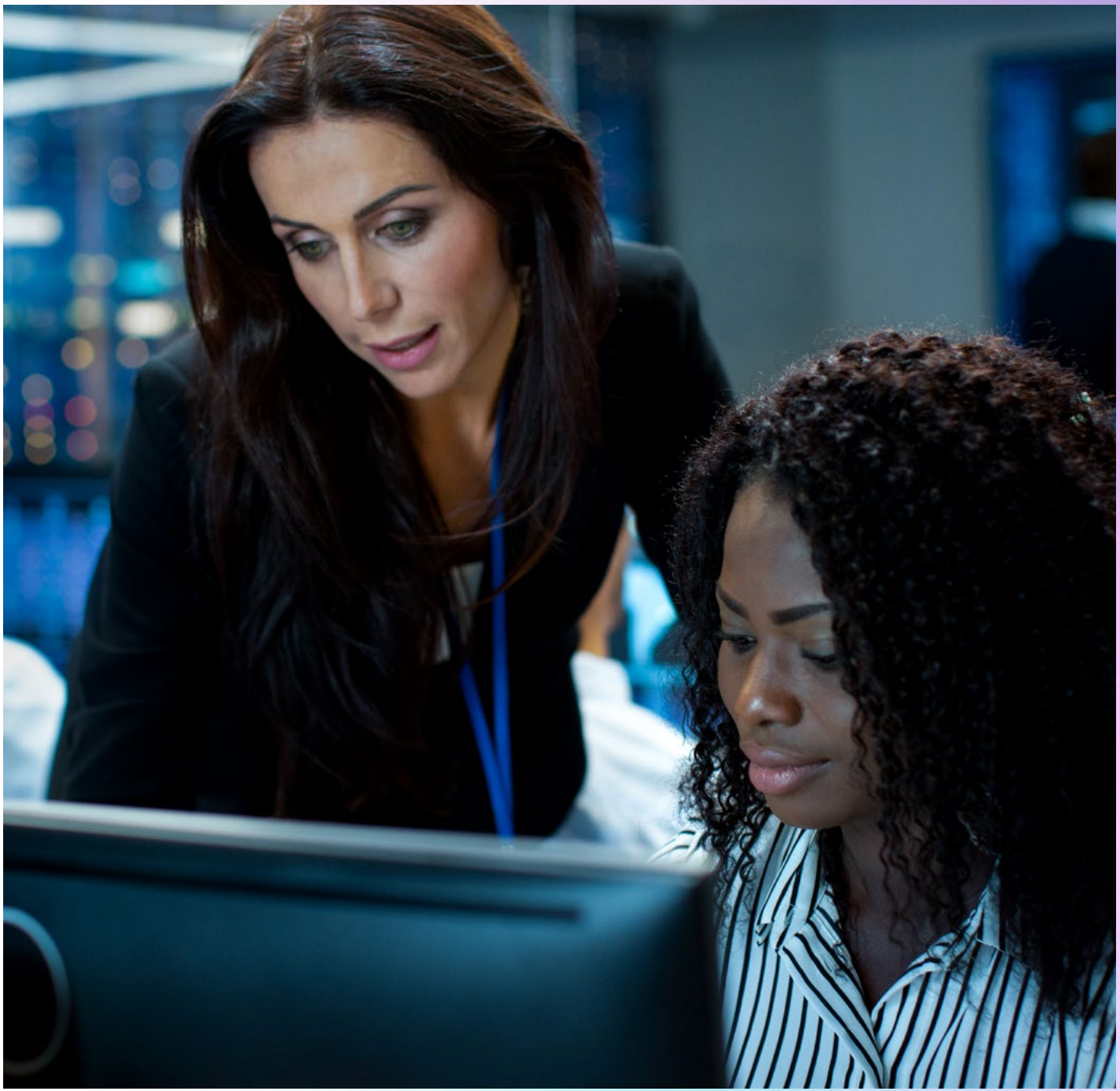
A robust approach to cyber-security should bring all your security efforts together, in one place. With threats this high, there's no room for a siloed approach.

It's just not going to be strong enough. And there's no point in solutions that only patch up parts of the infrastructure, leaving gaping holes ready for the attackers to exploit. With all the opportunities that are at stake in your delivery of the future of work, you need a solution that mirrors its importance.

Cyber-security is a 24/7 operation. It requires constant monitoring, regular reassessments of your security posture, evolving recommendations, and scalable capabilities. The goal posts are always moving, and you need to be ready for that. A trusted partner with an end-to-end service can apply a ringfence around your people, your workplaces, and your business. This will bring you full visibility and enable your people to get on and thrive in the job they are here to do.

BT Security directly responds to the challenges our partners face while alleviating budget and skills shortages. Our team of over 3,000 security experts will translate your business priorities into future-proofed security strategy. We have a unique view of the entire network with CREST accredited intelligence capabilities (and access to Interpol and NCSC global intelligence). And our use of automation and AI enables us to rapidly identify and predict cyber-attacks.

Every part of our end-to-end service works hard so you can move faster than your adversaries. It's designed to give you the confidence to embrace new technologies and drive your digital transformation. Because you know that behind the scenes, every second of the day, your entire cyber-estate and security strategy is being taken care of by a team of experts with the most sophisticated intelligence and technology.



Conclusion

While digital transformation puts businesses on a sure path to greater productivity, effectiveness, and growth, doing this securely is paramount.

A combination of cyber-security intelligence access, technical experience, and trusted security solutions will secure workforces, workplaces, and businesses – now, and in the future.

The government has been clear that security sits at the foundation of the UK's political and economic ambitions. Its new National Cyber Security Strategy provides the direction and investment required to maximise our capabilities. And with the help of BT's end-to-end service, enterprises can transition and transform their future of work to provide resilience in a constantly evolving security landscape.

I'd encourage us all to look at how innovation can challenge and accelerate every element of our security approach. To truly achieve this and do more than simply race to keep up with the latest threats, we must innovate in everything we do, not just technology. If we can do this collectively, we will advance the UK's global standing and the reputation of our organisations internationally.

To learn more about protecting your people, workplaces, and business, give us a call on 0800 7076313 and visit us here.

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

© British Telecommunications plc 2020. Registered office: BT Group plc | One Braham | Braham Street | London | E1 8EE. Registered in England No. 1800000.

June 2022