Managing multi-cloud security risk

How do organisations overcome the unexpected security risks of the multi-cloud to unlock its full transformative benefits?

Introduction

Turbulent winds of change have buffeted organisations over the past few years, disrupting operating models and how they are secured. Pandemic impacts, the shift to hybrid working and volatile economic pressures create a significant challenge: how can organisations navigate this in an effective, yet cost-conscious way?

A multi-cloud approach offers the more flexible infrastructure that fits with how organisations want to work today. Choosing clouds based on what makes the most financial or operational sense for each situation allows for dynamic and tailored responses to evolving situations – and creates opportunities to pull ahead from competitors However, this multi-cloud operating also brings new security risks that can't be ignored.

As a result, organisations need to reassess their multi-cloud strategies through a security-conscious lens to make sure every advance in agility, innovation and cost-management they make is fully protected.

It’s a complex, multi-cloud world

Organisations globally have embraced multi-cloud, with **87% of organisations** currently operating a multi-cloud model[1].

This isn’t surprising because the multi-cloud approach increasingly reflects the way that many organisations are looking to operate now and into the future. By embracing a multi-cloud strategy, organisations are looking to achieve a range of benefits.

Increased flexibility

In the multi-cloud, organisations can flex up and down with greater ease – resizing their consumption and costs based on their evolving requirements at any given time.

Enhanced resilience

Operating multiple clouds provides organisations with a more resilient infrastructure. They can also avoid cloud concentration that puts them at the mercy of a single provider’s decisions, outages, or security vulnerabilities.

Competitive pricing

Across the multi-cloud market, organisations can choose the most competitive provider for each specific job and avoid the constraints of vendor lock-in.

Clouds for specific workloads

Organisations have the freedom to take what they want from different clouds, selecting them based on what’s most suitable for a particular workload or operation.

Improved cloud connectivity proximity

Multiple cloud locations allow companies to select the zones that are nearest to their own locations.

Data sovereignty compliance

Many cloud service providers are providing sovereign cloud offerings to respond to governments increasingly enforcing data sovereignty requirements on organisations operating in their jurisdictions.

[1] Flexera State of the Cloud report 2023

State of the Cloud 2023: What's shaping different organisations' cloud strategies today?

Flexera's State of the Cloud 2023 report found that the most common reason for the use of a multi-cloud architecture was that organisations' apps were siloed on different clouds. This would suggest that decisions taken early on in many organisations' cloud journeys have had lasting effects on their architectures and future policies – while also creating long-term implications for their security posture.

The report also found that, while an increased number of organisations are using public cloud only, nearly three-quarters of respondents reported operating a hybrid cloud model – using a mixture of public and private clouds. Unsurprisingly, this split is more pronounced in enterprises that have 50% of their workloads in public cloud, compared to SMBs with 67%. This reflects the additional complexity in enterprise environments.

Five challenges in securing the multi-cloud

Despite its increased flexibility, the multi-cloud environment also broadens an organisations' attack surface, bringing a range of additional and unexpected security concerns for many organisations.

1. Uncertainty around shared responsibility and regional compliance

Getting to grips with the subtle distinctions between different providers and their varying requirements can be enormously challenging. This is because each cloud provider has a different model for defining the security responsibilities of both the provider and the customer, with small nuances between them.

This makes things like implementing efficient data governance and compliance measures across multiple clouds complex because some providers believe it's the customer's responsibility to understand and adhere to the varying data protection laws in different regions.

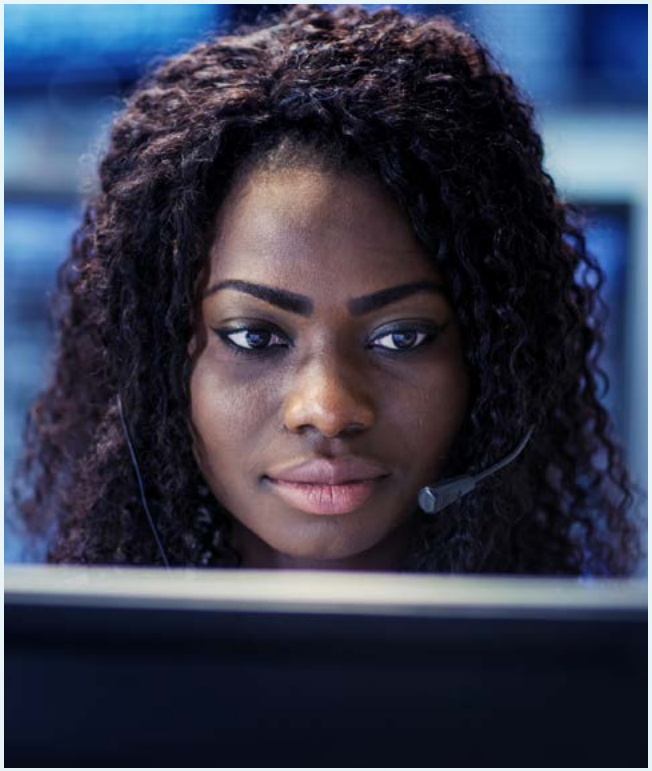
2. Lack of consistency across security policies and the potential for cloud misconfigurations

Each cloud provider has their own unique architecture, security standards and controls and management tools and configurations. This makes it challenging to enforce uniform security policies and maintain a consistent security posture across different cloud platforms.

Interoperability and integration challenges can also arise when trying to make different cloud services work together seamlessly. Managing multiple vendor relationships and contracts can be time-consuming and complex and, without dedicated resources and expertise, it can be very easy to make mistakes.

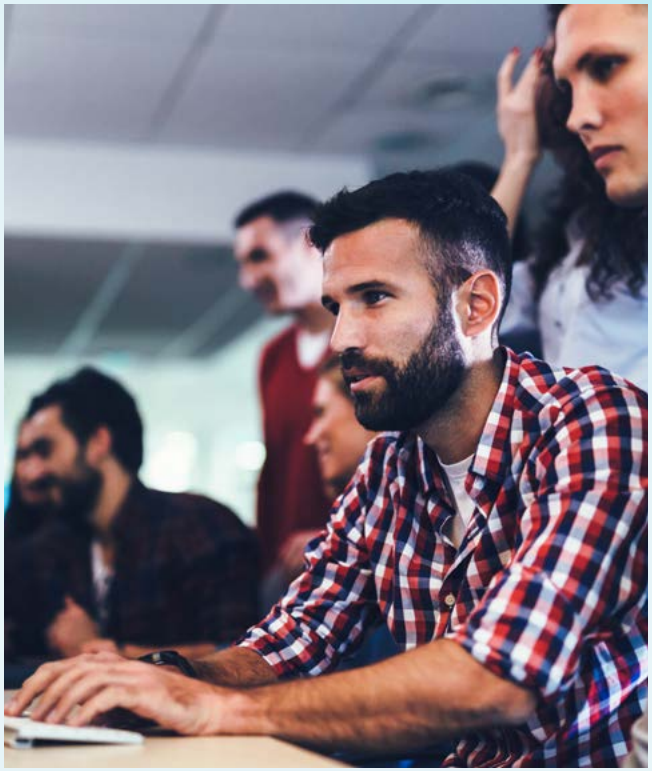
3. Demand for new cloud-based security measures

Many businesses haven't re-imagined their security approach for the cloud or sufficiently developed an inclusive cloud security architecture. Instead, they've simply chosen to extend and adapt their existing perimeter-based tooling and processes. But these legacy security controls aren't suitable for the dynamic nature of multi-cloud deployments.



4. Loss of visibility

Establishing comprehensive visibility across various cloud platforms is another significant challenge. If security teams can't achieve a unified view across all their cloud environments, then detecting and responding to security threats can be extremely difficult.



5. A shortage of cloud skills

There's currently a huge demand for people with the advanced cyber skills needed to meet the complexity and volume of threats in the multi-cloud. The continuous launches of new cloud features are also leaving already stretched teams to play catch up as they struggle to find people with the skills to understand complex cloud architectures.

How to address these challenges

Building a robust multi-cloud security stance is a stepped process that begins with a deepened understanding of the environment together with a shift in mindset, and then layers in standardisation, visibility, monitoring and automation capabilities.

1. Understand the nuances of the shared responsibility model

At first glance, the cloud security shared responsibility model seems simple to understand. The cloud service provider is responsible for the security 'of' the cloud, while the user is responsible for security 'in' the cloud. However, when it comes to multi-cloud security, it's important to dive a little deeper.

There can be important distinctions between SaaS, PaaS and IaaS cloud models, and communication between them can occur at differing levels of responsibility. Many organisations have workloads that require multiple types of cloud services, so understanding how the security controls for these services interact is fundamental. Each cloud provider will have their own shared responsibility security model, and there's a risk of gaps in functionality where security tools don't overlap. A brief look at just three hyperscalers demonstrates this point.

AWS: In AWS, customers are responsible for securing things like data, user accounts and the applications they host in the cloud. AWS are then responsible for securing the digital and physical infrastructure that runs AWS cloud services. But, depending on the services used, responsibility on the customer side may also include guest operating systems and firewall configuration.

Azure: In Azure's case, customers are always responsible for data, securing devices and managing accounts and identities. After this, the responsibility varies depending on the cloud model used but, generally, the more advanced the implementation, the more responsibility the customer must take for the OS and physical infrastructure.

Google Cloud Platform (GCP): GCP's shared responsibility model is the most complex – describing itself as 'shared fate' rather than shared responsibility. This model 'builds on the shared responsibility model because it views the relationship between cloud provider and customer as an ongoing partnership to improve security'. This can be especially tricky for the customer because understanding security responsibility when using GCP requires an in-depth understanding of each service. Customers are also required to understand the correct regulatory requirements of the business they're working in, as well as geographic differences. Although, under their shared fate model, Google does provide comprehensive guidance and security tools to assist with this.

Building up this understanding of how shared responsibility models can mesh together can be complex, and many organisations benefit from bringing in expertise to achieve this. A highly pertinent aspect of this expertise can be mapping out how different clouds meet the specific regulatory requirements of different regions.

2. Start managing cloud governance and access and standardising security policies

Enforcing a consistent, centralised global security policy across a multi-cloud infrastructure can be very difficult to navigate. A good starting point is to think about standardising your approach to security policy, while making sure it's also platform agnostic.

As we saw from the shared responsibility model, customers should, at the very least, expect to always be responsible for securing their data in the cloud and the access policies for that data. But, according to the Cloud Security Alliance, cloud misconfigurations are the third highest threat to cloud computing[2]. This highlights that, even at this level, customers are finding it challenging to navigate all the tools and configuration options available.

Some critical first steps to cover all cloud platforms would be to define data classification and categorisation policies and then implement appropriate security measures for each category. Customers can then control who has access to specific resources, services, and data by using granular identity and access management capabilities.

[2] Cloud Security Alliance Top Threats to Cloud Computing: The Pandemic 11
[3] Gartner: The Future of Network Security is in the Cloud. Neil MacDonald, Lawrence Orans, Joe Skorupa, published 30 August 2019

3. Evolve your legacy security mindset

Gartner's influential report 'The future of network security is in the cloud[3]' states that digital business transformation has inverted the enterprise. This means more work is now performed off the enterprise network than on, and more workloads are running in the cloud than in the enterprise data centre – resulting in decreased effectiveness in traditional perimeter security controls. Since its publication, we've only seen this trend accelerate, meaning that legacy security controls are now even less suitable for protecting today's dynamic secure access requirements. Robust defences in the multi-cloud world depend on taking security as close to the user and the workload as possible. The aim is to limit lateral movement throughout workloads and clouds using a Zero Trust approach. Core to this are Zero Trust network access methodologies, and host-based security controls that use a dynamic access policy to manage access at a granular level by workload.

4. Look at regaining visibility and improving monitoring

As the old saying goes, 'you can't protect what you can't see'. Multi-cloud architectures embody this problem due to the varying levels of log availability and access.

One of the ways organisations are addressing this is by implementing a company-wide centralised cloud team or Cloud Centre of Excellence (CCOE). Typically, CCOEs are responsible for managing and optimising cloud costs and cloud usage policies, selecting cloud providers, planning cloud migrations, and automating policies to govern cloud use. This can help to prevent shadow IT and unprotected workloads.

By bringing the monitoring data from all clouds and data centres together into a single location, organisations can gain visibility over their complete environment. This approach also helps address the problem of configuration drift – that is, the tendency of cloud setups to diverge from policy over time as changes are made. Monitoring and protection can also be addressed with technology solutions such as Cloud-Native Application Protection Platforms (CNAPP). These platforms aim to address workload and configuration security by scanning them in development and protecting them at runtime. A CNAPP includes multiple technologies, combining the capabilities of existing cloud security solutions such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP). It also includes Cloud Infrastructure Entitlement Management (CIEM), API discovery and protection, serverless security, and more.

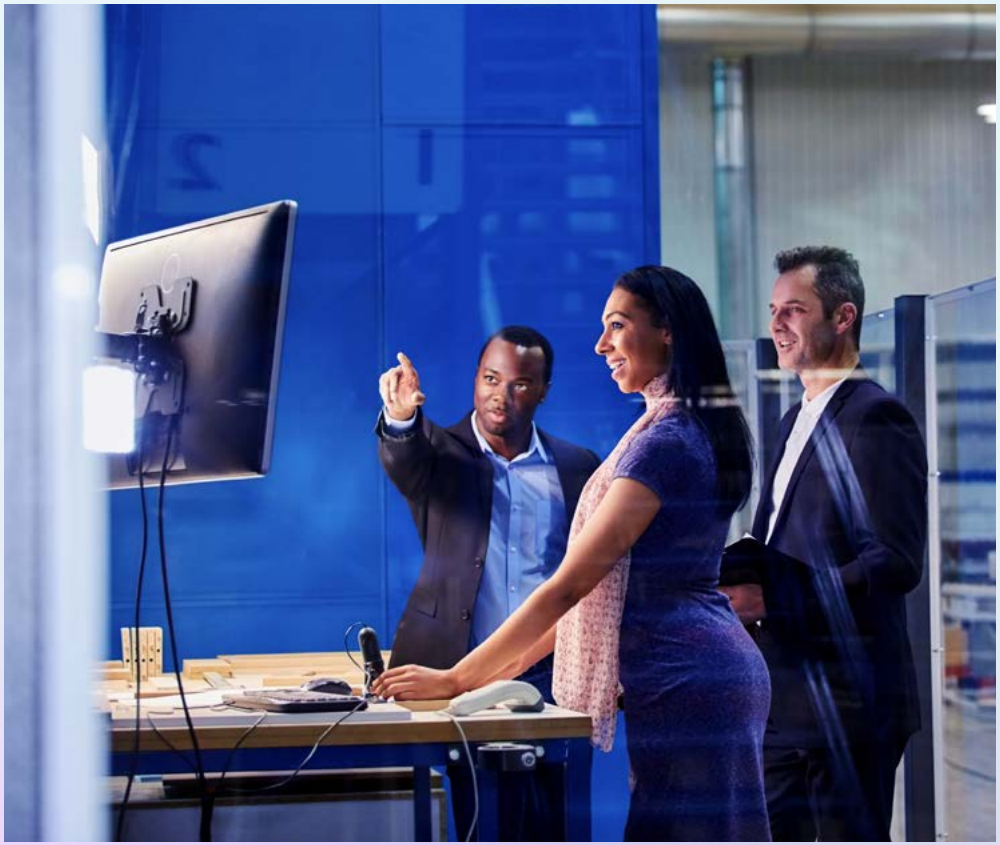
5. Explore implementing automation

A fundamental premise of cloud is that it's API-driven, which means that all interactions with cloud functionality can be authenticated, automated, logged and analysed. Finding ways to automate configuration, policy enforcement and vulnerability scanning and to introduce security earlier in the development cycle, can all contribute to a more secure-by-design approach.

Additionally, the speed with which cloud services can be launched, as well as the rapid advancement of cloud functionality, necessitates an automated approach. Some of the benefits of automating cloud security include speed and accuracy of detection, scalability across environments, robust compliance, and prompt alerts to threats – all of which lead to considerably improved security.

When it comes to threat detection and response, a widening attack surface coupled with an increasing number of security tools means that most organisations' security teams can easily become overwhelmed. There are often so many alerts coming in, that they struggle to identify the right ones to focus on. Addressing this often involves bringing in external expertise to support on systematic review and change, or as an ongoing managed service.

Automation can also play an important role in solving this by triaging and automatically remediating low-level threats, freeing up human analysts to focus on the more critical and complex alerts.



How networking and security can work together to secure a multi-cloud approach

Multi-cloud networking can be complex and, as organisations increasingly invest in cloud fabric infrastructures, it's important to consider networking and security together. One example of this is Secure Access Service Edge (SASE), which combines SD-WAN with cloud-delivered security.

Of course, different organisations have different needs based on their business objectives and also have differing maturity levels, risk appetites, vertical sector and existing controls. This makes an early assessment of what's important to them, and what they're specifically trying to achieve, critical.

Bringing it all together: how we can help

We know that customers are at different stages of their multi-cloud journeys. It's clear that some haven't fully re-aligned their security approach for cloud while others haven't developed their cloud security architecture and merely extended and adapted their existing controls and processes. But, regardless of where you are, we can offer targeted help to meet key needs.

Manage the complexity

With us, you have a trusted partner on your side to navigate the complexity of a multi-cloud environment. We can help you understand the wide range of cloud security solutions on the market, as well as what embedded security with different cloud hyperscalers could offer. We'll make sure you have the right security, in the right place, at the right time, and maintain your security posture as new threats and vulnerabilities emerge.

Enjoy a tailored service specific to your needs

Our Security Advisory Services team has years of experience in supporting customers with their cloud security architectures. They work with you to understand your current investments, how they can support your multi-cloud journey and identify any gaps you may have. They can also incorporate modern security architectures such as Zero Trust and SASE, while focusing on the specific needs of your organisation.

Take a multi-layered approach to security

From ensuring the identity of your users and OT / IoT endpoints, to protecting your data at rest and in transit, our layered approach provides you with a comprehensive multi-cloud security approach that brings together defences of the clouds themselves, and what goes on within those clouds. It also ensures you can meet your confidentiality, availability, and integrity requirements.

Make the most of our extensive cyber security experience

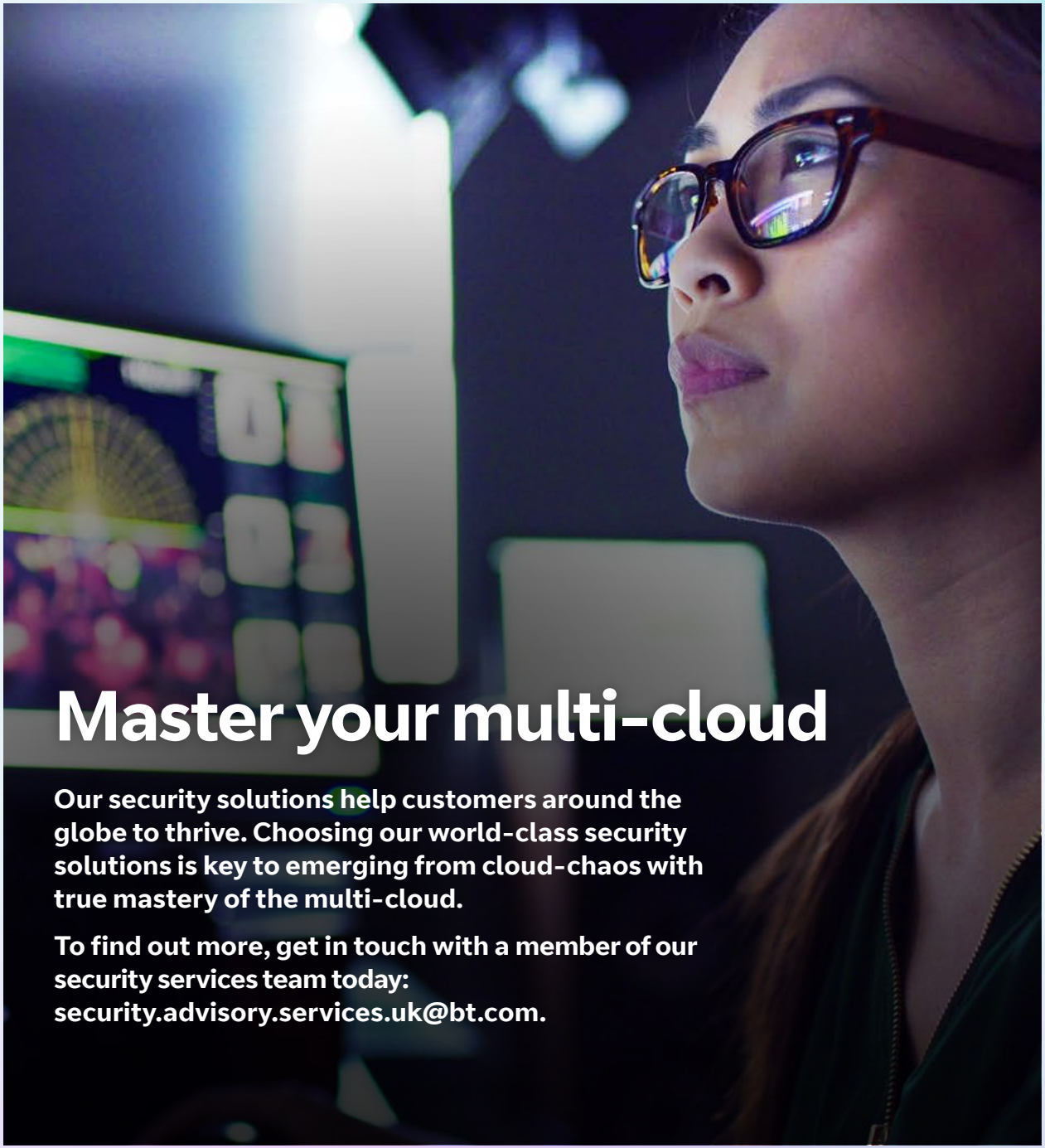
We've been securing ourselves and our customers for over 70 years. We understand that robust security is not just about providing you with technology, it's about combining it with our people, processes and expertise to help you stay secure. Our team of 3,000 cyber security professionals deals with around 6,500 cyber attacks a day. And our customers directly benefit from our strong partnerships with organisations such as Interpol, the National Cyber Security Centre and worldwide ISPs. This combination means we uncover threats early and then use this information to protect our customers, giving you valuable time to co-ordinate your responses.

Use our wide portfolio of multi-cloud solutions

Our portfolio delivers both breadth and depth of functionality from our global security partners, covering both security controls and threat detection and response. All these solutions are then covered by our graded managed service wrap that's managed through a single web portal, freeing up your team to concentrate on higher value activities. We can address your security needs at all points in your infrastructure – from network underlay to overlay, CNF to private and public cloud, right through to your endpoint, identity, and data security.

Look to the future

Our sophisticated Eagle-i cyber defence platform combines our network insight with advances in AI and automation to provide real-time issue detection and intelligent, automated responses. The platform self-learns from the intelligence provided by each intervention, so that it constantly improves its threat knowledge and dynamically refines how it protects customers across a multi-cloud environment. It's also able to integrate with technologies from across the security ecosystem, so you can choose best-in-class solutions to fill gaps in your capabilities, and integrate them with your existing investments.



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.

October 2023