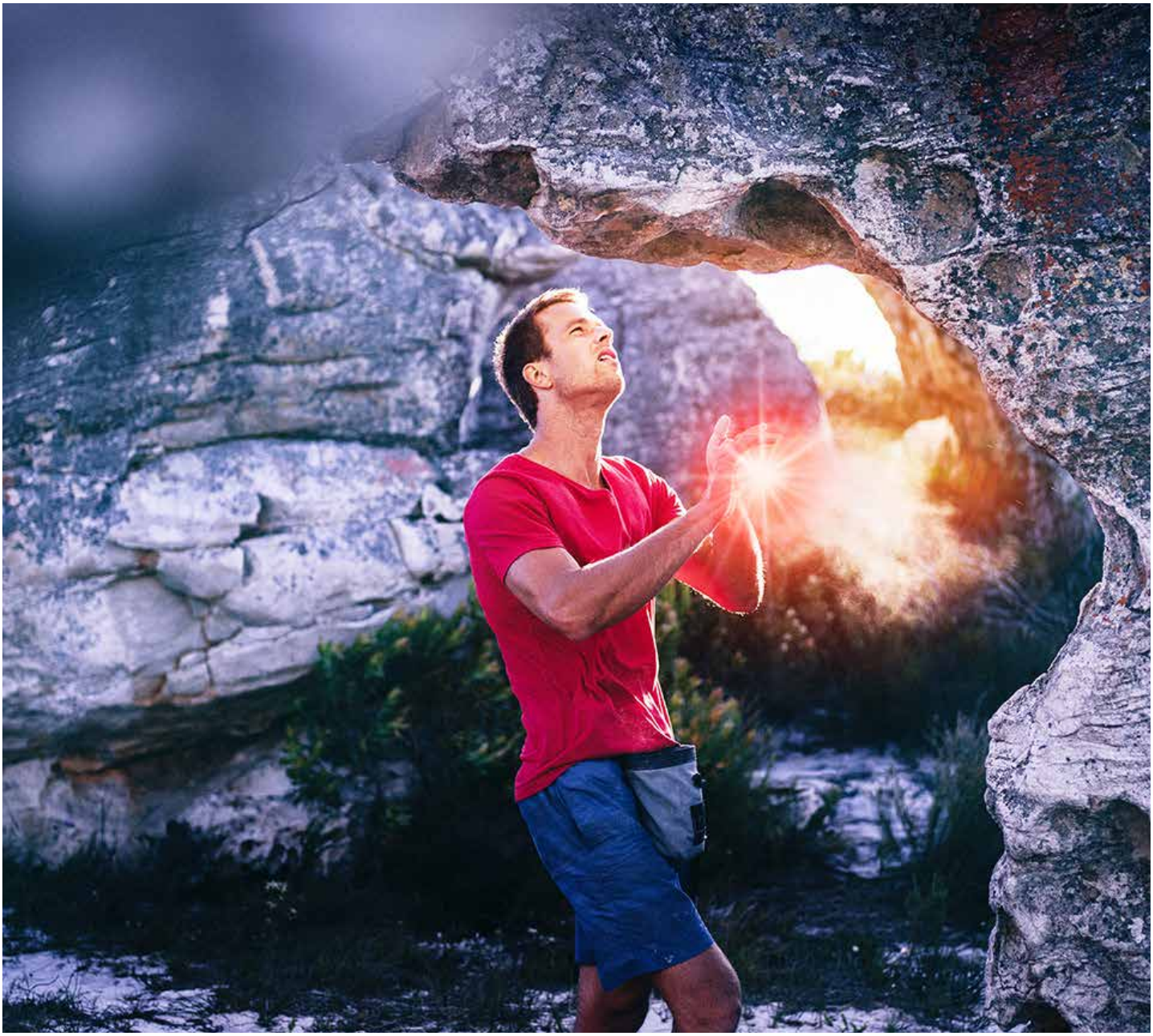
FUJITSU

White paper

The rise and rise of multi-cloud brings huge opportunities and new security challenges: Fujitsu has solutions

Moving into the cloud does more than help businesses keep ahead of evolving customer demands, digital competitors or new regulatory requirements.



Introduction

Moving into the cloud does more than help businesses keep ahead of evolving customer demands, digital competitors or new regulatory requirements. It also lets organizations tap into a wealth of cloud-driven opportunities for innovation and business growth. In fact, the typical enterprise today relies on many cloud services to streamline and automate processes, improve agility and roll out new capabilities quickly.

That multi-cloud approach to business presents new challenges – especially in security. When each cloud service provider offers its own administrative and security tools, managing multiple cloud services can quickly become complex. And that complexity can lead to siloes, limited visibility, inconsistent application of controls, or unexpected and undetected gaps in enterprise security, creating new, potentially costly risks.

If your organization is facing this, Fujitsu can help. Our unique combination of skills, services and technology experience lets us reduce complexity and achieve the right balance of capabilities in a multi-cloud environment. We enable enterprise customers to effectively manage security risks, optimize investment and improve operational efficiency. And our global reach and large portfolio of security technology partners lets us implement solutions for companies across industries and geographies. Read on to learn more about today's multi-cloud security challenges, and how we can help you manage those more effectively.

Welcome to the multi-cloud future

It wasn't that long ago that many businesses were reluctant to move to the cloud, often because of security concerns. But cloud services have evolved since then, adding enterprise-class security, wider support for compliance and other advanced capabilities. As a result, more and more enterprise organizations now embrace the cloud. In fact, the vast majority often uses many different cloud services at once, for many different business needs – payments, supply chain management, sales, enterprise content management and more.

The trend is expected to continue: 86% of the market reports a cloud-first or cloud-only policy. So, cloud is clearly still the core foundation of IT and business strategies.[1]

Benefits

The cloud makes it easier for enterprises to move into the digital business era. It makes it possible to adapt services as needed to respond to fast-changing customer demands. It can improve efficiency. It can reduce costs. And it provides flexibility and agility in a world where technologies and regulations are continually evolving. It's easy to see, then, why multi-cloud use is on the rise.

Most multi-cloud users today rely on a blend of private and public cloud solutions. The average user has nine cloud vendors in all.[2] Among cloud-only enterprises, that number rises to 13. What's more, the number of cloud-only organizations has doubled in the past year.

Challenges

So the multi-cloud strategy clearly dominates among enterprise users. However, with its many benefits come new challenges. In a 2018 Fujitsu survey, senior IT decision makers reported growing difficulty in keeping up with rising demands, both from customers and from internal stakeholders. They also said they were finding it harder to create new digital services, manage suppliers and manage multi-cloud architectures.

There are other challenges too. With the vast and growing selection of cloud services to choose from, more users say it's hard to know which solutions to implement. And they're finding it difficult to integrate multiple cloud services, provide a consistent experience for their users and ensure visibility for governance and compliance.

A Fujitsu survey[3] found the number-one concern respondents cited – named by 95% – was security.

Getting security right, it turns out, is a key enabler for moving to the cloud. And a balanced security strategy is even more critical for organizations using multiple cloud services at once.

How multi-cloud affects security

While security in cloud services has matured, users must still be alert to cloud threats, risks and vulnerabilities. That's particularly true for organizations using multiple cloud services.

Cloud security presents different challenges because the platform extends the potential attack surface far beyond the traditional internal and external threats facing an in-house data center. It's no wonder that more than half of IT leaders surveyed said their cloud estates have become too complex to manage properly, and that they lack the in-house skills needed to do so.

When an organization moves services into the cloud, the IT department loses part of its usual gatekeeper role. Different units of the business can now easily buy any number of as-a-service solutions without needing to give much thought to data security precautions or policies. And the deployment of multiple cloud services brings an assortment of cloud-native security controls, which can be used differently and inconsistently across different parts of the organization. All of this presents oversight and governance challenges, making it difficult for IT to apply security policies consistently.

Data breaches are always a concern. When cloud defenses are misconfigured or defeated, it can lead to unauthorized access and compromise of sensitive or protected data. This can result in a loss of customer trust and reputational damage, as well as financial harm from fines and lawsuits.

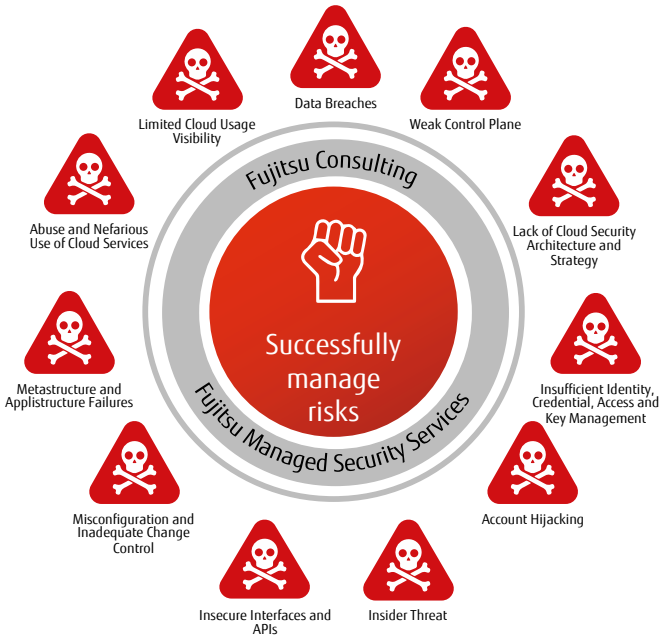
Poor control over cloud assets can also pose a problem. Misconfiguring cloud services, or not protecting them well enough, can make it easier for people to access information and applications they shouldn't have access to.

[1] "The state of orchestration 2018/2019" p. 8, Fujitsu, https://www.fujitsu.com/uk/imagesgig5/driving-a-trusted-future-research-report-uk.pdf

[2] "The State of Orchestration 2018/2019," p. 9, Fujitsu, https://www.stateoforchestration.com/app/data/3361_FUJ_Orchestration_Report_2CS_AW_10DEC.pdf

[3] Ibid

Cloud Computing Risks



Source: Cloud Security Alliance (CSA)

11 risks

Data breaches and poor control are just two of the risks that the Cloud Security Alliance cautions against in its list of the 'Egregious Eleven'.

While each of these risks exists for any individual cloud service, managing them becomes far more complex for a multi-cloud enterprise user. That task is further complicated as cloud services are updated or changed, which happens often – every few days, if not more frequently – with the typical service.

Keeping secure in a multi-cloud world

Fujitsu's approach toward multi-cloud security tackles challenges across three pillars: internal threats, external threats and cloud threats. We work to help enterprise customers clearly understand their risks and security posture across all three pillars, and to present solutions that protect availability, confidentiality, data integrity and resilience.

We also address critical security considerations related to compliance. This is particularly important in heavily regulated industries such as finance or healthcare. Remember: even a fully compliant organization is not necessarily a secure one.

Moving into the cloud isn't a simple 'lift-and-shift' exercise. It's important to consider the complexity of the applications. And any migration plan should evaluate all options. This includes re-platforming for cloud optimization, to ensure there are tangible benefits from moving to the cloud. Refactoring might also be required. This involves re-architecting and developing an application to use cloud-native features.

A transition to the cloud requires organizations to address a variety of security concerns up front, and to understand the value and sensitivity of the assets they're putting into the cloud. It also means working with a shared responsibility model, in which the cloud service provider is responsible for a secure infrastructure, while the organization remains responsible for data security. Whatever service is deployed, enterprises should always aim for security by design.

All of the above holds true whether an organization is using one cloud service or a dozen or more.

Let's look at how such security works – internally, externally and in the cloud.

Internal threats

While cloud service providers are responsible for the security of their platforms, enterprise users are responsible for securing their assets in the cloud. To do this, they need to configure systems properly, protect against insider threats, address regulatory compliance requirements and otherwise stay on top of internal security demands. This includes keeping alert to changing security needs – because those needs are guaranteed to change over time.

For example, enterprise cloud users must watch out for misconfigurations or excessive permissions that could leave data vulnerable to malicious activity. Other potential weak spots include improperly set default credentials, lapses in patching, disabled logging or monitoring activities, and unrestricted or unexpected access to ports and services.

Managing access, credentials and identities is especially critical. While this is true on or off the cloud, staying secure becomes much more difficult if an enterprise has to manage multiple identities for each user in a multi-cloud environment. Any insider with authorized access to internal systems can pose a threat – intentionally or not – when sensitive data and applications are moved onto the cloud.

External threats

In a multi-cloud environment, protecting against external threats also becomes more complex. That's because cloud services can be accessed online by anyone with the credentials and privileges to do so. This increases the potential for harm by malicious actors who find their way in, whether via an account takeover, social engineering or malware.

There's also an increased risk that cloud computing resources can be hijacked to threaten an organization from the outside. This opens the door to a range of other potential threats: distributed denial of service attacks, 'cryptojacking' that uses cloud resources to mine for cryptocurrencies, email spam and phishing campaigns, automated click fraud on a massive scale, the hosting of malicious or pirated content, brute-force attacks powered by databases full of stolen credentials, and more.

Cloud threats

And then there's the variety of challenges posed by the cloud itself. These include everything from issues with visibility and managing changing workloads to dealing with multi-tenancy concerns and choosing between cloud-native or cloud-agnostic security and support services.

Settling on the right security architecture is especially important with public cloud. And, whatever support cloud services offer, enterprise cloud users need to recognize they will always have shared responsibilities for security.

Again, moving data and services to the cloud involves more than a simple transfer of tasks once handled in house. For instance, accessing cloud services via the internet requires the use of software user interfaces and APIs. If these are poorly designed or poorly protected, they could open the door to unauthorized users and increase the risk of a major data breach.

Duplicating, migrating and storing data also becomes more complex in a multi-cloud environment. Not all cloud services store and manage data in the same way. Without proper integration between them, it can be difficult to coordinate threat intelligence and collate indicators of a data breach or malware threat. And if you are spreading redundant copies of your data across multiple clouds, how will you keep all that data in sync?

Done right, security controls for managing infrastructure in the cloud – the control plane – can ensure such tasks are handled properly. A weak control plane, on the other hand, can leave administrators, systems architects and engineers with gaps and blind spots. Such weaknesses can increase the chances of data corruption, unavailability or data leakage.

Another challenge for enterprise users with multiple cloud services involves the choice between cloud-native or cloud-agnostic security. Cloud-native security may be the best choice for a business using just one cloud service. A multi-cloud organization, on the other hand, might benefit from taking a cloud-agnostic approach that is effective – and also easier to manage – across all of its services. We'll look at this challenge in greater detail later.

Identity, access management and encryption

Tackling all of the above challenges in a multi-cloud environment requires an enterprise view and understanding of security. Fujitsu takes a holistic, multi-layered approach to this. And one key focus area involves how we manage identity, access and encryption.

Our digital identities today are the most important asset we have. A bad actor who hijacks someone else's identity can wreak havoc, online and off. In the business world, a misused or hijacked identity can lead to lost data, lost customers and costly organizational damage. In the cloud, identities have become the new security perimeter.

Fujitsu believes a business can strengthen security by ensuring each user has just one identity across all cloud services. And a centralized and effective identity management regime can make security even stronger: it enables enterprises to easily add users and grant them access to the services they need to do their jobs. It also lets them grant new access rights when employees gain new responsibilities, and withdraw access rights completely when people leave the organization. We support organizations with identity as a service and provide identity and access management as a managed service to our customers.

Without centralized identity management and a well-defined 'joiners, movers and leavers' process, there's a risk a sign-on event could slip through the cracks and allow an ex-employee to access corporate systems. Centralized management also enables oversight of systems administrators and other privileged users who could access sensitive data and applications or change permissions to allow unauthorized users to slip past defenses. Fujitsu's Privileged Access Management as-a-service (PAMaaS) offering provides strong authentication for individuals who use privileged accounts, leveraging single sign-on and granting controlled access to target systems in accordance with predefined access rights and policies.

Data itself also requires special security considerations in a multi-cloud environment. Whether it's traveling across a network or being stored at a service provider's data center, data must be protected against unauthorized exposure. The best defense here? Encryption. This reduces the risk of someone seeing something they shouldn't, even if other defenses fail. For example, even if unauthorized access is gained to a shared cloud platform, an enterprise user can be confident its encrypted data will remain secure and inaccessible.

Multi-cloud security considerations

Shared responsibilities

Depending on the type of cloud services used, an enterprise customer will retain various responsibilities even as the cloud service provider takes over others. In this shared-responsibility model, users are typically in charge of customer applications and data, as well as network security, identity and access controls, data encryption and operating systems/platforms. The cloud service provider, meanwhile, handles compute, storage, database and networking services on the cloud platform, and manages other aspects of its global infrastructure.

For organizations in a multi-cloud environment, understanding these shared responsibilities and managing them effectively is vital.

Fujitsu can help enterprises manage these responsibilities through its multi-layered, holistic approach toward multi-cloud security. That approach supports customers across many different configurations, not just organizations with a large number of cloud services. For example, we can help smaller businesses currently in a single-cloud environment to grow correctly from the start, so their future evolution into a multi-cloud environment can take place without compromising security.

Our model for delivering these services covers the full range of cloud security concerns – identity and access management, data protection, endpoint security, threat management, security monitoring and more – through a combination of both technical and strategic consulting. Working on our own and with trusted third-party partners, we help our customers develop security measures that provide compliance, continuity and resilience.

Our approach ensures organizations can mature their operations in the cloud and build strategies and architectures that are effective over the long term.

Cloud-native vs. cloud-agnostic security

Enterprise users need to give thought to finding the right balance of security in the cloud. This involves analyzing their requirements and options with a long-term view in mind. Some organizations might need support with this. Security consulting can help them identify needs and implement an effective strategy. Other businesses might already have clear ideas about what they need and will choose to evaluate a number of security controls, including those available natively, against a detailed set of requirements.

As a business expands into an ever-larger number of cloud services, however, that decision becomes more difficult. An enterprise with a dozen different cloud services – including a mix of IaaS, PaaS, SaaS, FaaS (function as a service) and serverless models, as well as different data storage and backup services – could find itself working with multiple security controls across the organization, highlighting the need to ensure support for consistent security processes. Achieve this by enhancing individual cloud services to meet common, business-wide security requirements.

Opting for a cloud-agnostic approach to security can also pose obstacles, though. Cloud-agnostic means security controls are interoperable and can be applied across any number and variety of different cloud services. But managing such a system across all of an organization's cloud services is complex, and not every enterprise is up to the challenge. And the risk of not applying controls consistently – or missing critical gaps and vulnerabilities – rises with every new cloud service added to the mix. Fujitsu recognizes the pros and cons of cloud-native versus cloud-agnostic services will vary, depending upon how and where such services are used. Our expertise enables us to help businesses find the right balance of security controls to meet their unique requirements.

There are other considerations too. Businesses in highly regulated industries might prefer to retain complete control over security by choosing their own security solution over a cloud provider's native service. This might be because they need complete control over their data, or because they want to operate in a hybrid IT environment as their approach to risk means some of their sensitive or regulated data must stay on-premises.

Organizations with complex systems are likely to have a substantial investment in traditional IT and may have mainframe or other non-x86 environments that don't easily transfer to public cloud. Opting for a cloud-agnostic approach might be more pragmatic for these organizations due to its greater flexibility and portability should the need for cloud services change.

Any organization should consider where it makes sense to use cloud-native security controls – remembering of course that these can't be used in cloud services from other vendors – and where it might be a better option to use a third-party, cloud-agnostic solution that can be deployed across multiple clouds.

Fujitsu has a wealth of experience in this area, as well as a global reach and a large number of technology partners that can help, whatever an organization's situation. We have worked with numerous enterprises navigating multi-cloud environments to develop strategies that are right for them.

Private and public cloud concerns

As organizations increasingly move into a multi-cloud environment, they're using both private and public cloud offerings. While private cloud usage has a slight edge in adoption – 58% vs. 42%[4] – public cloud adoption is growing. Cost and scalability benefits are among the reasons for this. For example, users that will usually opt for a public cloud service could include an airline seeking the flexibility to handle an increase in user traffic online when their new flight schedules are released. Or a tax authority that needs to handle a last-minute rush in tax returns at the end of the year. Or even an online pizza delivery company that anticipates a surge in demand during a major sports event.

The pros of public cloud flexibility, however, come with some cons, particularly around security. When an organization sits in a public cloud, it shares space with multiple customer tenants. And if one tenant has less-than-ideal security, other organizations in that cloud space could also be at risk. Your organization is dependent on the logical isolation controls the cloud platform provides.

For businesses in highly regulated industries, public cloud might not be an option for certain applications and services. And that means an enterprise must pay even closer attention to due diligence when selecting a cloud service provider.

Fujitsu's wide expertise in both public and private cloud deployments allows us to assess a variety of enterprise needs to identify the right security solution.

Cost considerations

The number of organizations with multi-cloud environments is growing because of the considerable cost benefits that approach offers. Yet if they're not handled properly, security concerns can put a dent in those cost benefits.

Look, for instance, at managing workloads with cloud-native encryption. An enterprise going that route could face a costly and difficult decision if it needs to move its assets to another cloud service provider: such a move could require the user to first decrypt all of its data, then move it and re-encrypt it in the new cloud environment.

Providing security in a multi-cloud environment via a single-sign-on user experience can also be challenging. Such a system, if it's poorly designed and implemented, could end up being complicated to operate, as well as costly.

Fujitsu knows how to help customers overcome such obstacles. We have deep experience in integrating and provisioning applications, both on premises and in the cloud. We also offer identity as a service, which lets enterprises deploy identification, authentication and access solutions quickly, easily and cost effectively.

[4] "The State of Orchestration 2018/2019," p. 5, Fujitsu, https://www.stateoforchestration.com/app/data/3361_FUJ_Orchestration_Report_2CS_AW_10DEC.pdf

Conclusion

To achieve the right balance of security in a multi-cloud environment, enterprises must take many things into account. One critical consideration is identity and access management, which encompasses privileged access management, identity lifecycle management, identity administration and governance. Other matters to think about include encryption, cloud-native vs. cloud-agnostic security, shared responsibilities for security, threat management, endpoint protection, reporting requirements, compliance and more.

Finding the right solutions across all of these areas can be a complex exercise. And making the wrong choices can leave an organization with misconfigured systems that are difficult to manage, or risky – and potentially costly – security gaps.

With Fujitsu's expertise and holistic, intelligence-led approach to cloud security, we can help enterprises more easily and securely manage their multi-cloud environments. We assess each customer's security needs and challenges, and work with them to transform their security posture, create visibility, and enhance intelligence, predictability and their ability to react. We then help them to continually evolve and improve to optimize security.

In addition to our delivery capabilities and our comprehensive portfolio of technology solutions, we also provide both technical and strategic consulting services. With early engagement through our independent consulting capability, we help customers to define their cloud security strategy and understand their compliance requirements. Our extensive cyber risk management experience gives our customers the confidence that their multi-cloud environment is secure. And we work with numerous leading third-party security partners whose solutions complement our own, allowing us to address virtually any security need an organization might have.

With a global presence and more than 40 years of business experience, Fujitsu is ready to help your organization find the right answers to its multi-cloud security questions. And as an independent consultant, we don't promote any single service provider or technology: our aim is to work with our customers to find the solution that works best for them. Our main goal is to help you achieve an outcome that optimizes your organization's security in the cloud, and ensures your long-term business success.

Contact
Ask Fujitsu
+44 (0) 123 579 7711
askfujitsu@uk.fujitsu.com
@FujitsuSecurity
Ref: 3938

www.fujitsu.com/global