Intro

There are many reasons that an organization may need to engage a cloud security company. It could be to harden their environment, perform penetration testing, complete a security assessment, or assist with architecture design. One of the most common reasons is that an organization is in the early stages of its cloud adoption or infrastructure transition. This is the most critical time for an organization, as it will set many of the constructs, controls, and processes that will be followed for the foreseeable future. Building a secure environment from the beginning will not only ensure that the organization is protected but will also prevent the build-up of technical debt that will need to be addressed later.

When it comes to cloud computing, many different platforms are available. It is not just Azure, Google, and AWS but others like Oracle, DigitalOcean, and many other lesser-known brands from which to choose. Due to many vendor options and the complexity that resides within each environment, it is important to engage a firm that has experience with the platform you are operating. Consultant companies may have experience with more than one cloud provider, so it is not a one-to-one relationship.

The Best Cloud Security Companies in the US

Many of the world’s cloud solution providers started in the US market. Just like any other security service in the US market, there is no shortage of consulting companies and vendors that will claim to have experience in cloud security. Some of these companies do, but some just add the service to their list of capabilities, even though they are limited. True cloud security is not about taking the existing architecture and virtualizing it in the cloud. Many capabilities are built into the cloud provider that can help streamline and improve security. It is about weighing which of the cloud services will be utilized vs. third-party tools.

**Optiv**

Optiv is one of the largest security providers in the world. Even with that, they continue to focus on what their clients need and that includes cloud security. With its large base of consultants, partnerships, and tools providers, Optiv can assist any company at any maturity level with its cloud security needs. Whether it is an evaluation of tools, deploying new tools, testing, or assessments, Optiv has the service and ability.

**Coalfire**

Coalfire is best known as a PCI auditor. However, they have a strong technical skill set outside of PCI and are known for working with some of the largest cloud solution providers. With this working relationship, a deep understanding of compliance frameworks, and a strong technical team, Coalfire would be a great partner in building out the initial cloud architecture and controls for any organization making a transition.

**LogicWorks**

LogicWorks is positioned with a strong set of skills in AWS and Azure. They offer many services that are geared towards cloud service providers, including security. This is a shift from some of the other companies discussed in this article. With the ability to provide services outside of security for a company, LogicWorks is positioned to be your one-stop provider for cloud migration, cloud build, or cloud posture assessment.

**Microsoft, AWS, Google**

These three are almost a gimme for any list, which is why they are all grouped together. Many organizations fail to realize that all three of these companies offer up security services in some form or fashion. While Microsoft may have the most mature approach to providing services, having a fully formed consulting service business unit, they all offer something. Any one of them can be engaged to assist with assessments, architecture design reviews, operational questions, and even deep dive presentations into tools and capabilities (both native to their platform and third party). When looking for a vendor to assist, do not hesitate to contact your cloud solution provider for help.

The Best International Cloud Security Companies

When it comes to international cloud security companies, there are quite a few that can be leveraged. Some are region specific, while others are global and operate both in the US and internationally. In fact, in recent years, there has been an expansion of service providers working internationally, especially in Europe. Some of this is related to data privacy and an increased emphasis on data security, while other reasons include continued globalization.

**Accenture**

Based out of Ireland, Accenture lands on the international company list. While most people would assume their presence is just in the US, this is not true. Accenture has resources nearly everywhere a client may require them, along with a strong understanding of local and regional regulations, laws, and standards. Accenture works with some of the largest companies in the world, and even some of the cloud providers themselves. Due to their vast experience and numerous engagements, Accenture has a wealth of knowledge and internal capabilities to assist your organization with the transition to the cloud.

**IBM**

IBM has a large consulting arm that is globally positioned, much like Accenture. While they have their cloud solution, they are also known as an integrator for companies looking to be multi-cloud. This positions them to assist with highly complex cloud security architectures that are not limited to just one provider. Additionally, IBM has multiple tool investments that can provide additional value for engaging them for a security service.

**KPMG**

KPMG is best known as a CPA firm providing services on the financial side. However, they have a very large certification, audit, and security services arm that operates strongly across the board. KPMG has grown its global presence through both organic growth and acquisition. This has allowed them to pick up markets in Australia, the Netherlands, and many other countries in recent years. While KPMG may not be as well-known on the cloud services side as other vendors, they are still readily capable to assist.

Best Boutique Cloud Security Companies

When looking for a partner for cloud security and cloud infrastructure consulting, size should not deter your organization. There are many vendors and service providers out there that are small but still possess strong technical skills and a track record of success. When looking for one of these vendors, look for one that has certified partners or that has been recommended to your organization. When it comes to the cloud, some of the best security practitioners are working for smaller boutique companies.

**CyberSecOp**

Offering services across security, CyberSecOps has built a strong cloud security practice through partnerships and consultant skills. With a focus on Azure and AWS as their primary cloud infrastructure vendors, CyberSecOps has built a strong offering to assist organizations with design, building, and improving security architecture and controls in the cloud. Further, they have also started to transition into offering up services to assist with security SaaS cloud solution providers.

**Hybrid Pathways**

Founded with the cloud in mind and assisting organizations with their transition to the cloud, Hybrid Pathways has continued to focus on providing value to organizations through adding security services. With the focus on designing and building secure architecture, Hybrid Pathways looks to build a repeatable process for their customers. With consultants that have worked with Fortune 100 companies in varying capacities, Hybrid Pathways brings the ability to meet the largest organization’s needs in their venture to the cloud.

The Best Value Cloud Security Companies

I did quite a bit of research this week and just am not comfortable with providing any value vendors in this space. Too many of them felt sketchy or just adding the service for a money grab. I can continue to look if you like, just let me know,

Tips on Choosing Cloud Security Companies

Whether your organization is planning a migration to the cloud, mid-cloud transfer, or has been operating in the cloud for some time, selecting the right partner is critical. As mentioned, there is no shortage of vendors that claim to have cloud security expertise, but this does not always hold water. Many will just look to shift existing on-premise architecture to the cloud, which can lead to poorly managed and optimized cloud deployments. In most cases, organizations are looking to transition to the cloud for flexibility and speed, not to replicate their existing architecture. So, when it comes to looking for a partner with your cloud security, below are some tips to consider.

**Expertise**

This may appear obvious, but it seems to be overlooked all too often. A strong relationship with a vendor or a partner does not mean they will be the best choice for you. Consider which cloud providers the existing or potential partner has expertise in. This can be accomplished by questioning if any of the consultants on staff are certified in those environments, how often they work in that specific cloud service, and if they use that provider. Further, if you have some knowledge of that cloud hosting provider, ask the vendor specific questions related to those solution tools, capabilities, and platforms. After all, the way that an Azure environment is going to be configured and managed will be completely different than how AWS will be managed. Having some experience in other cloud providers does not always mean it will correlate to your provider.

**Experience**

When speaking to your potential vendor, inquire about what kind of cloud security projects they have led. If you are just beginning your journey, discussing a vendor’s solutions around managed services may not make sense. If you are further along in your journey and looking for managed services, discussing solutions for building a secure architecture may not make sense. The reality is that not all vendors can offer solutions across multiple maturity levels. Some vendors excel at helping to operate a more mature cloud deployment, while others are fantastic at designing and building a new environment.

**Compliance**

In many cases, organizations looking to shift to the cloud are looking to make sure that their compliance posture stays intact. So, why not make this a core requirement to evaluate vendors? The reality is that not all auditors understand how the cloud works. Your organization needs to be able to not only design and implement a secure control but talk in depth about how this relates to compliance requirements. A great example is related to PCI, it requires network firewalls to be implemented for all environments. Does this mean a virtual firewall must be installed in your cloud environment, or are there existing capabilities within that provider that can be positioned as the same capability? This is just one example of where finding a vendor that understands your compliance frameworks and requirements can assist with not only deploying the right security tools but also building the story for your auditors and customers.