About the author

Melanie Jones is product director for cyber security portfolios at Global Knowledge (www.globalknowledge.com), where she has worked for over 15 years. She is responsible for managing the strategic vision, product portfolio planning, innovation and go to market strategy. Jones manages technology portfolios in collaboration, datacentre, cloud, security, IoT and big data analytics, as well as being a product lead for cyber security portfolios for EC-Council, CompTIA, CQURE, ISACA, (ISC)2 and SECO. She is a member of key Cisco, collaboration, cyber security and big data groups worldwide.

References

1. '2019 IT Salary and Certification Report'. Global Knowledge. Accessed Apr 2020. www.globalknowledge.com/en-gb/forms/2019-it-salary-and-certification-report.
2. '2020 Cloud Security Report'. Cybersecurity Insiders. Accessed Apr 2020. www.cybersecurity-insiders.com/portfolio/cloud-security-report-prospectus/.
3. '2019 Cost of a Data Breach'. IBM/Ponemon Institute. Accessed Apr 2020. https://databreachcalculator.mybluemix.net/.

A multi-cloud world requires a multi-cloud security approach

Rory Duncan

Rory Duncan, NTT UK

We are increasingly living in a multi-cloud world. According to the '2019 Risk:Value Report', over a third of respondents in global organisations say their company currently stores its data in a shared or public cloud environment, such as Amazon Web Services (AWS), Microsoft Azure or Google. Around the same proportion stores data in a private cloud. These numbers are set to go up as more and more businesses transition their processes and applications to the cloud.

A multi-cloud strategy sees an organisation leveraging two or more cloud computing platforms to perform various tasks, using resources from several providers to reap the best benefits from each service. This gives the organisation the flexibility to choose the service that best suits its needs, and it's often the case that organisations will use different cloud providers in different parts of their business, or for different use cases.

There are many well-documented benefits of multi-cloud – businesses can enhance their customer and user experience, improve staff productivity and deliver cost savings by moving from a capex to an opex model. Additionally, organisations can enjoy the benefits of agility and scale while improving resiliency, availability and performance.

Increasing risk

Malicious actors are always looking to capitalise on new attack vectors, using cloud infrastructure to launch and execute attacks. Data and application sprawl and possible misconfiguration of cloud infrastructure are among the vulnerabilities that can expose data to attacks. Transitioning to the public cloud also involves a transfer of responsibility and control to a third party – the cloud service provider (CSP) – with the potential for mis-management, loss of governance and ambiguity over responsibilities.

Protecting data, defending against potential threats, maintaining compliance and securing workloads across all cloud environments requires a holistic security strategy. Securing the multi-cloud means managing the challenges of data everywhere, including multiple cloud identities and mobile connections. There's no one-size-fits-all or simple fix, but organisations can avoid introducing additional complexity and risk if they begin by gaining a full understanding of their multi-cloud environment, and the data and threats encompassed within it. This visibility will be their starting point for a practical and prioritised roadmap for building security into cloud deployments.

Better visibility

It is essential to have a complete picture of the infrastructure, information assets and flows, workloads and applications residing across all cloud environments. Organisations need absolute certainty on what data they have, where it is stored, how it is accessed and used, and by whom.

The value and importance to the business of each service, application and data asset then needs to be determined, so that the organisation can ensure the appropriate security controls are in place. It also needs to conduct a proper risk assessment to establish the base level of security required and ask itself what level of risk it is prepared to accept for those resources to be delivered from the cloud.

The security posture

In a multi-cloud estate, it is critical for an organisation to maintain or exceed the level of security and privacy protection it had in its traditional IT environment. To understand where security capabilities need to be bolstered, it needs to find out what controls are in place and whether or not its cloud environments meet legal and regulatory requirements.

This should include a formalised and consistent approach to assessing the security of the CSP. Security capability and service levels vary between cloud providers. While leading vendors have invested heavily in their security infrastructure, some do not possess even the most basic native security controls such as two-factor authentication, encryption and strong password enforcement. API-based security and the securing of various remote endpoints, for instance, are often simply not catered for.

It is important to establish what sort of cloud providers are in the ecosystem, and whether their native controls are aligned to the organisation's security policies and fully address its risk appetite. If not, additional security controls will need to be implemented – either by the provider or by the organisation as part of the deployment.

Any business that is working in the cloud must acknowledge that it cannot entirely delegate responsibility for data integrity and protection. Cloud security is a shared responsibility between the organisation and each of its cloud providers.

Security responsibility

In general, the cloud service provider is responsible for securing the cloud itself, while the customer is responsible for protecting its data and controlling access to that data. Even leading cloud service providers such as AWS and Microsoft Azure have made the limits of their responsibility for security and compliance very clear by defining a model of shared responsibility.

To ensure that information security is managed appropriately throughout the information supply chain and service lifecycle, organisations and vendors must agree and document a strong, clearly defined and aligned security governance framework. This should set out the specific security requirements on both sides to mitigate any risks associated with infrastructure, applications or data. It should also outline how the security of the cloud service will meet compliance standards and how ongoing risk management will be demonstrated. The organisation – not the CSP – should be defining service levels, and any service should be an extension of its current security policy, maintaining existing levels of confidentiality, integrity and availability.

Once the organisation has a full understanding of what users are doing in the cloud, established its attack surface and pinpointed where its weaknesses lie, it's time to look at which native and third-party controls will most effectively protect the multi-cloud environment.

Apps, data and infrastructure

Security in the cloud requires a multi-layered and data-centric perimeter that protects information with relevant controls. As a minimum, these should incorporate:

- Data encryption.
- Multi-factor authentication.
- Privileged identity and access management controls.
- A next-generation firewall.
- Application container security.
- Anti-virus software.
- Vulnerability management, to ensure that applications are being patched.

Effective security incident management is also essential, to enable real-time threat detection and response. Organisations must be prepared and have a plan in place for how they will manage such incidents, using analytics across the multi-cloud environment to detect threats, vulnerabilities and configuration weaknesses.

Secure by design

Irrespective of where an organisation is on its cloud journey, it's unlikely that its cloud deployments will ever stand still. New workloads will be moved to the cloud, and the business will want to take advantage of new capabilities and services to support its goals. It is therefore important to create a culture of continuous improvement, to ensure that cloud security grows alongside cloud deployments.

A 'secure by design' approach should be integral to all cloud services and applications, to enable businesses to be agile in the face of a changing threat landscape and technology ecosystem. This approach involves designing a security architecture that ensures that security is built in, rather than bolted on. Consistent security control mechanisms are applied across the board – at the point of developing systems, processes, services and applications – aligning processes, tools and technologies across an entire multi-cloud environment and the supporting IT infrastructure.

Organisations will continue to transition their processes, applications, and workloads to the cloud. Weaknesses or gaps in security controls within a multi-cloud estate can lead to myriad problems, from security incidents not being discovered, to reputational damage or loss of revenue. A holistic cyber security strategy will help to mitigate the risks inherent in a multi-cloud environment, while enabling the organisation to reap the business and technology rewards associated with it.

About the author

Rory Duncan is security GtM leader at NTT. He has over 20 years of experience within the IT security industry. In April 2006, he joined Dimension Data and became leader of the UK security business. In his current position his role is to drive the go-to-market strategy for cyber security in the UK and Ireland.

Reference

1. 'Risk:Value 2019'. NTT. Accessed Apr 2020. www.nttsecurity.com/docs/librariesprovider3/resources/2019-risk-value/ntt_gbl_riskvalue_report_2019_uea.pdf.