Adoption of cloud computing is at the heart of most organisations’ digital transformation strategies.

Cloud computing promises increased flexibility, scope for scalability, automatic updates and simplified collaboration.

On the way to achieving these benefits, organisations face an array of new security challenges:

- Obscured visibility into users, data and applications.
- An endless stream of technology changes that security teams must stay on top of.
- Increasingly diverse ecosystem of employees and third parties using these services.
A Changing Security Landscape

An explosion of cloud-based applications and mobile devices has blurred old boundaries around organisations and network security resulting in a vanishing perimeter and increased focus on identity based user and device authentication.

To keep up with the pace of change, business users are adopting cloud services; bypassing IT to deploy the applications they need to meet their business objectives but consequently creating digital islands of data and potential backdoors into the network.

Yet how we access computers and networks hasn’t changed much—passwords are still the dominant user authentication method, and more complex passwords do little to combat identity theft, which has become the number one attack vector:

The 2019 Data Breach Investigations Report confirmed that not much has changed, 80% of hacking-related breaches still involve compromised and weak credentials.*

User Experience

78% of security professionals think the biggest threat to endpoint security is negligence among employees.*

User frustration with passwords has reached epic levels. Ensuring your authentication experience is both secure AND user friendly will discourage users from attempting to bypass your security controls. Consider these ways to promote user adoption:

Implement Single Sign On technology for a more user friendly experience. Logging into one central hub is more convenient for users which means administrators can apply more stringent controls such as Multi Factor Authentication or increased password complexity.

Consider Biometrics: It’s incumbent upon mobile manufacturers to establish a verifiable ID, so that application and service providers can extend levels of trust to a device and its associated applications. These devices can also be used for authentication.

Roll out Awareness Training: If end users appreciate why security controls have been introduced and how to identify threats, they are more likely to adopt secure working practices.

Authenticate cloud users, devices and other assets proportionate to associated risks. Endeavour to ensure that security does not negatively impact productivity by only authenticating when it’s necessary.

Ecosystem

86% of organisations describe their cloud strategy as multi-cloud.*

An organisation’s cloud ecosystem refers to the hardware, software, cloud providers, consultants, integrators and other third-party partners that work together to form an organisation’s extended cloud infrastructure.

As organisations move more workloads and data to the cloud, they grow increasingly dependent on third-party technologies and services to support their businesses. This, of course, increases complexity and widens the risk landscape. But the following actions can help you mitigate ecosystem risks related to your cloud transformation:

- Maintain a record of all the applications and services supplied by cloud providers.
- Classify and prioritise the criticality of both the data “handled” and the services provided by each cloud partner.
- Understand third-, fourth- and nth-party cloud relationships and their importance to your business.
- Define the resiliency requirements and assess the corresponding capabilities of cloud providers that support the delivery of critical services.
- Identify security vulnerabilities in cloud-based software and services and collect cyber threat intelligence on cloud-based attacks.
- Assess the potential business impact of service interruptions or outages for each cloud provider.

Shared Responsibility

Gartner predicts that through 2022 at least 95% of security failures in the cloud will be caused by the customers.*

When it comes to cloud security, cloud service providers and their customers frequently have conflicting ideas on who’s responsible for what. For example, one common misconception among organisations procuring cloud services is that responsibility for securing their data shifts completely to the cloud provider. In fact, it does not.

The following governance controls can help your organisation manage security responsibilities with your cloud providers:

- Define a comprehensive set of cybersecurity-related policies and procedures for third-party cloud service providers to follow.
- Establish a process for capturing and managing cloud provider relationships, their importance to the business and potential risks.
- Evaluate your cloud providers’ controls for data retention and disposition ensuring that they align with your organisation’s policies.
- Assess your cloud providers’ capabilities for monitoring and securing their physical and digital environments.
- Clarify who is ultimately responsible for different security issues, including declared security incidents.

Identify

Phishing attacks are exploiting the social networking aspects of cloud-based collaboration tools.

Passwords, static identity and access management rules don’t provide sufficient defence against attacks that take advantage of cloud vulnerabilities and the myriad of employees and third-parties who need access to cloud applications at any time, from any device.

Therefore, secure access to cloud applications requires a high level of assurance that users are who they say they are and that their access is appropriate given their responsibilities and doesn’t put the business in harm’s way.

While managing access has historically revolved around traditional identity and access management tools, today’s new cloud realities require organisations to go well beyond those basic controls to:

- Govern joiner/mover/leaver access rights for employees and third parties and manage credentials and entitlements for authorised devices and processes.
- Apply the principles of least privilege and segregation of duties when granting cloud access permissions and authorisations.
- Correlate data across multi-cloud environments to understand the potential risks associated with authenticating users and assigning rights.
- Continuously monitor user behaviour and activity related to connections, devices and software.
Compliance

A major European airline faces a record £183.4 million fine after personal details of 500,000 customers were exposed to cybercriminals.*

When it comes to regulatory compliance, organisations need to understand what types of data they have in the cloud and where that data resides.

With traditional on-premises systems, auditors can literally see where data is stored. IT can also restrict or segment data based on attributes like geography, group and data type.

In contrast, cloud computing relies on the ability to host data in multiple locations. Multi-cloud environments complicate data privacy and compliance even more because data simultaneously resides in multiple cloud instances. These may have different business purposes and may be bound by different contractual relationships.

Implementing the following compliance controls can help your organisation meet a variety of internal and external regulatory requirements:

- Classify sensitive data, identify where in the cloud it is stored, and assess the potential compliance implications of data location, collection and use.

- Continuously monitor and assess cloud data usage to ensure adherence to regulatory and corporate privacy standards.

- Regularly inform employees and customers about cloud data collection practices and the specific data being collected.

- Evaluate cloud providers’ controls related to audit/log records and how they are documented, implemented and reviewed in accordance with applicable regulations.

- Train employees and third parties on information security and data privacy regulations; make sure they understand their responsibilities for keeping data safe, including codes of conduct for handling data.

Conclusion

There are a number of key challenges and myriad of tools available to support digital transformation projects. Moving to the Cloud is akin to moving home:

- Why take clutter with you
- Make sure you are moving to a safe area
- Make sure you know who has the keys to the door

1. Take stock of users, applications, location and devices. So you have full visibility of what you are protecting.

2. Understand the impact and value of your data so you can prioritise and protect accordingly.

3. Put tools in place so you can control of your data, users and policies.

4. Introduce a strong identity based access policy in place for your users to protect your data and network.

For independent advice about how you can ensure your Cloud Transformation project is as risk free as possible please contact BlueFort on:

enquiries@bluefort.com
01252 917000
bluefort.com