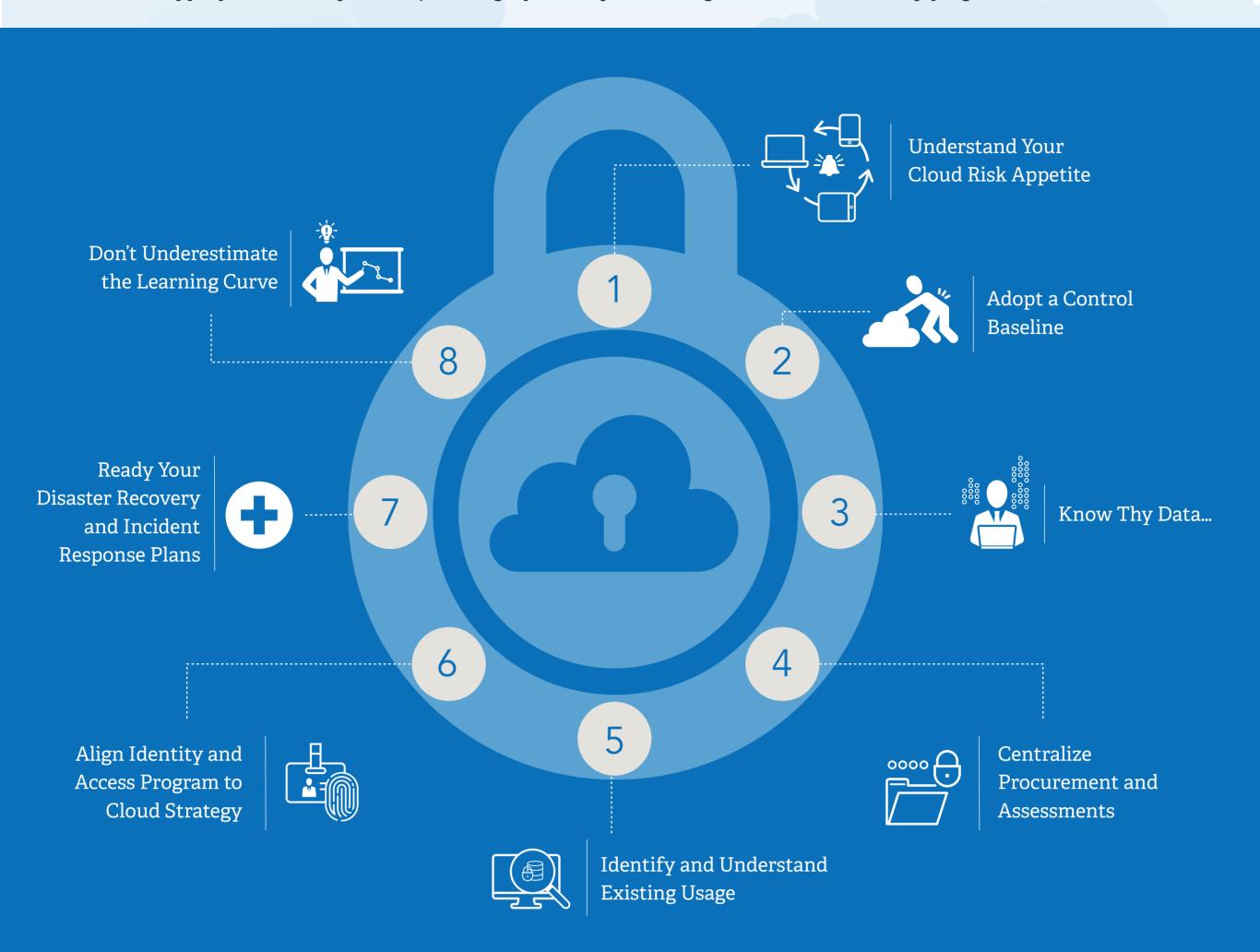
KEYS TO SUCCESS WHEN SECURING YOUR CLOUD ENVIRONMENT

To make the most of your move to cloud and protect your business, you must understand the associated risks and build appropriate security in. The following tips are key to building a robust cloud security program.



Learn How Optiv Can Be Your Key to a Secure Cloud



1: STRATEGY AND RISK ADVISORY

New cloud providers are entering the market at rapid speeds and often market features take priority over security.

It's up to the customer to perform due-diligence and add their own security layer.

The evolution to the cloud has accelerated the need to think holistically about security up and down the supply chain.



2: GOVERNANCE, RISK AND COMPLIANCE

With most cloud providers (IaaS, PaaS or SaaS), the responsibility of implementing and managing security changes falls on the customer. The less direct control a cloud consumer has over configurations, the less direct control they will have over the security

Considering industry standards and compliance requirements is a necessity.



3: DATA CLASSIFICATION

Without understanding the data living in the cloud, how can you best protect your organization?

Data classification leads to understanding the different types of data flowing through cloud applications and systems and allows for applying greater controls to sensitive or confidential data.



4: THIRD-PARTY RISK MANAGEMENT ADVISEMENT

Cloud services are frequently disparately deployed.

Organizations should drive to centralize all procurement activities through key departments and create criteria to assess the security risk of new and existing providers. Crucial organizational stakeholders from procurement to legal, security and IT are needed to ensure new cloud services are assessed uniformly.



5: CLOUD ARCHITECTURE CONSULTING AND CASB DEPLOYMENT

Differentiating between sanctioned, approved and unsanctioned services can be very difficult, as most cloud services can be accessed from anywhere.

It's important to implement the proper discovery and monitoring tools to help understand cloud application usage and to identify what is unknown and unsecured.

Understanding these assets assists in strategy development and securing the data.



6: IAM ADVISORY SERVICES AND WORKSHOPS

Organizations face numerous challenges when managing user identities and access requirements.

To truly secure the enterprise, only trusted employees, partners and consumers should access applications using trusted devices.

Identity and access management pulls together the disparate authentication methods that may be in place, simplifying managing accounts across cloud service providers.



7: STRATEGIC ARCHITECTURE AND INCIDENT RESPONSE SERVICES

Cloud service providers often have robust failover environments, but that doesn't mean your hosted instance has the same precautions. The deployment of cloud services has a tremendous amount of flexibility.

Undergoing a disaster recovery scenario ensures this capability is built into the design and validated in testing.



8: SECURITY AWARENESS TRAINING

Gartner predicts that leading up to 2020, 95 percent of cloud security failures will be user error, not the fault of the cloud provider.

Cloud service providers are maturing their security, but have key differences in their approach. These differences can interfere with how policies are applied within any given organization. Training on security practices as it relates to each cloud service should be required by users and administrators.

