



## WHITE PAPER

---

# DEVisING A SECURE CLOUD STRATEGY

# TABLE OF CONTENTS

# DEVISING A SECURE CLOUD STRATEGY

Whether you are already using the cloud or not, you should have a cloud strategy in place. And this strategy must closely align to the business' strategic initiatives and the strategic IT objectives that are intended to support those initiatives. If there is one word to describe the opportunities that exist within the cloud and how it can impact your business, it's "transformation," whether large or small. This is transformation not only for your business, but transformation or modernization for how IT does its business, and how security and compliance get done as well.



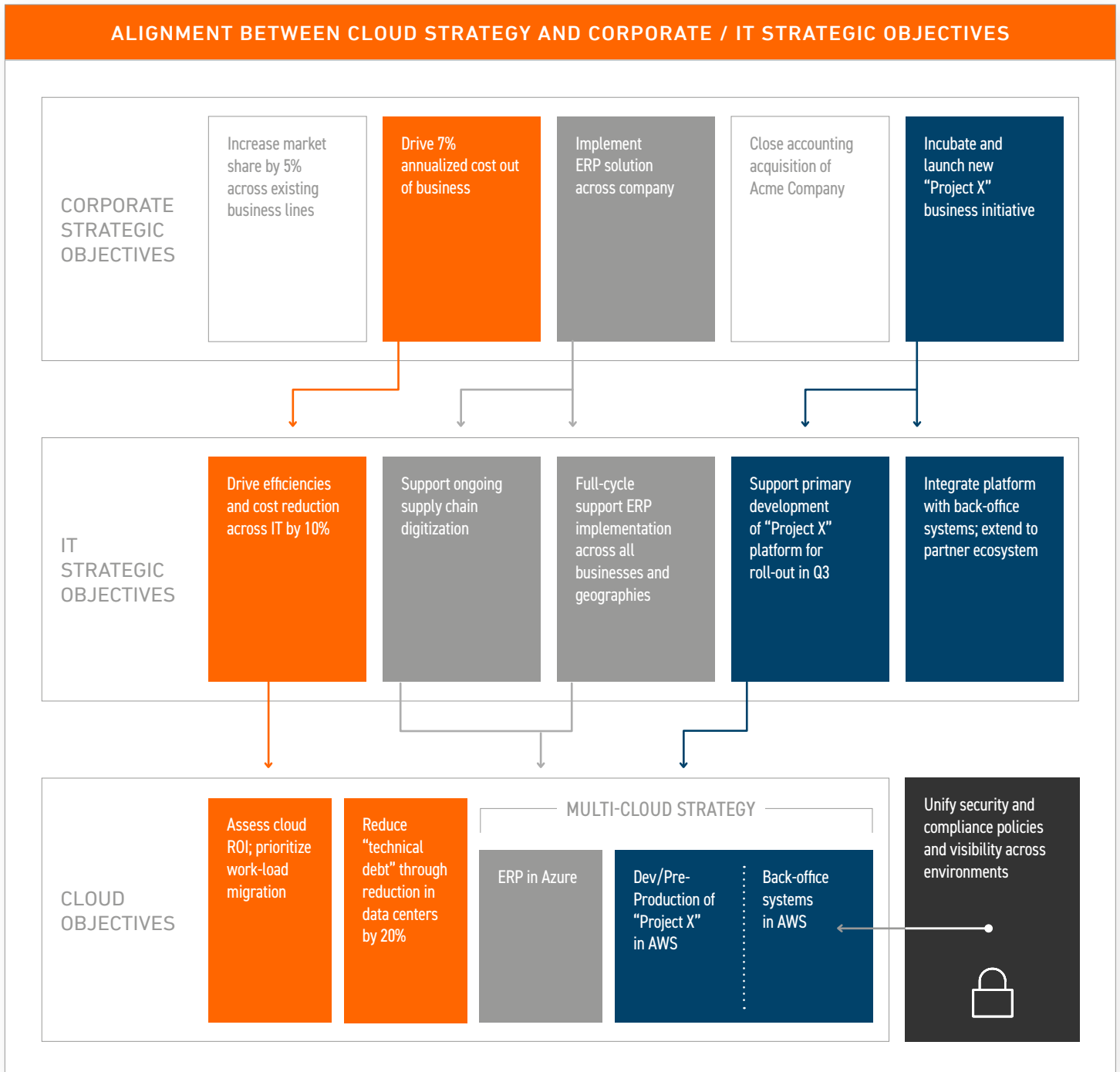
**If you aren't thinking about the transformative opportunities the cloud can enable, and that leaders might look to you to realize, you need to get a game plan fast.**

— Josh Bosquez, CTO,  
Armor



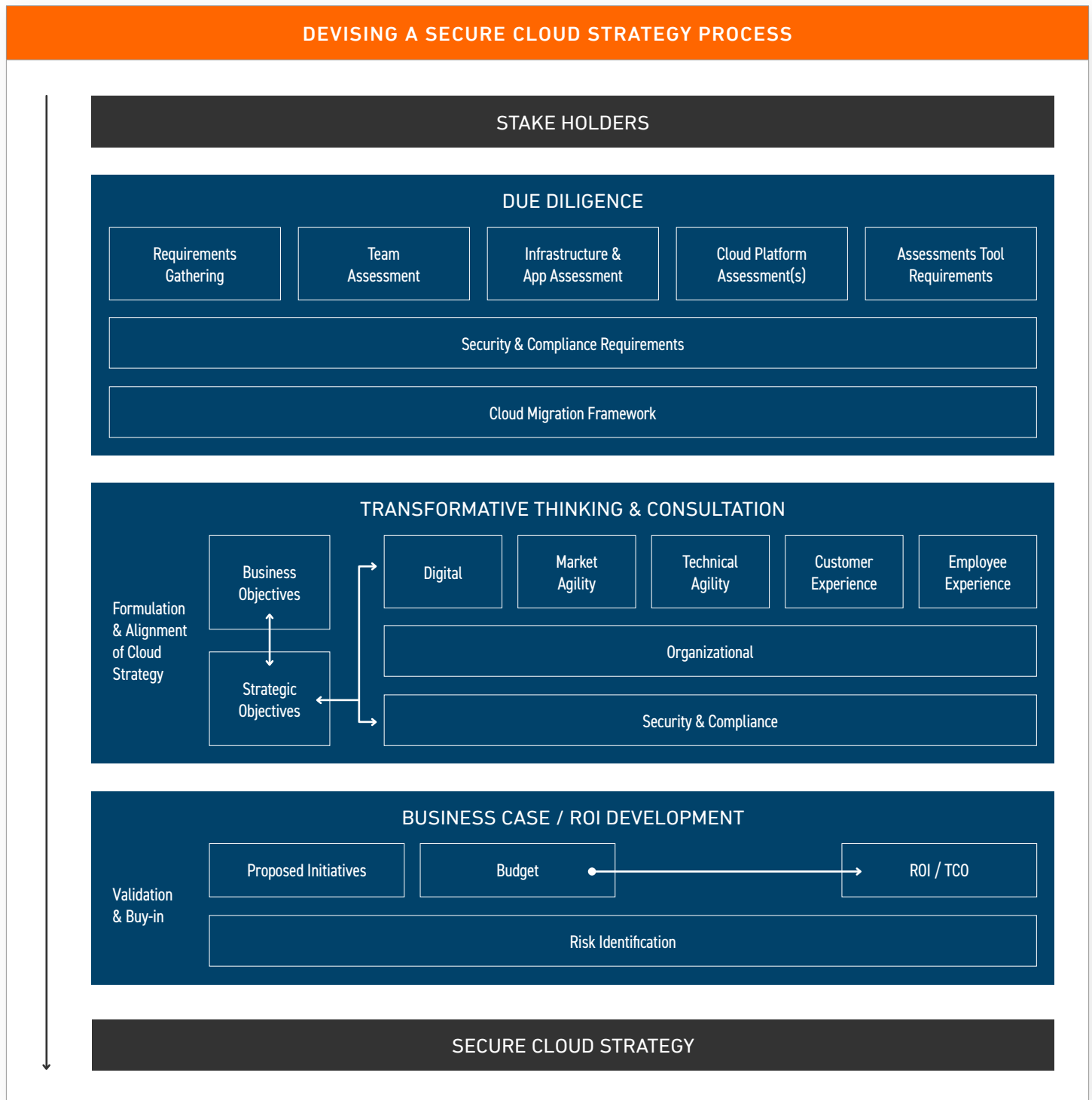
# STRATEGIC ALIGNMENT

Your ultimate goal in devising a cloud strategy is to enable the business' overall objectives and those of IT. Transformation and modernization represent the lenses through which your efforts, enabled by the expanding capabilities of public cloud platforms, are focused.



# HOW-TO

Devising a cloud strategy is a deliberative process that takes input from all areas of the business.



## STAKE HOLDERS

Stakeholders are the key to understanding objectives and needs across the business as well as winning consensus for your strategy. Leaders charged with developing a strategy for the cloud should expect to spend considerable time discussing needs with business heads as well as collaborating closely to identify opportunities for transformation and/or modernization.

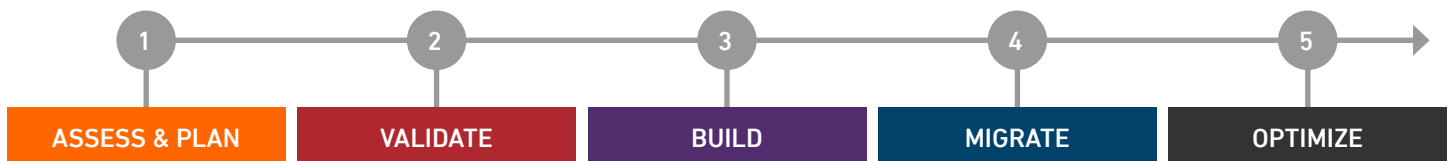
## DUE DILIGENCE

The quality of your efforts in the due diligence phase will greatly influence the success or failure of your cloud strategy. At this stage, it is important to select a cloud migration framework to guide your migration efforts. The fact is that the first stage of any migration framework includes many of the same activities necessary for formulation of your overall cloud strategy, as depicted below using the **Secure Cloud Migration Framework** as an example. You will want to conduct an inventory of your current environment(s); assess and prioritize applications and data in terms of importance or business impact; investigate cloud platforms and their capabilities; and capture security and compliance requirements along the way.

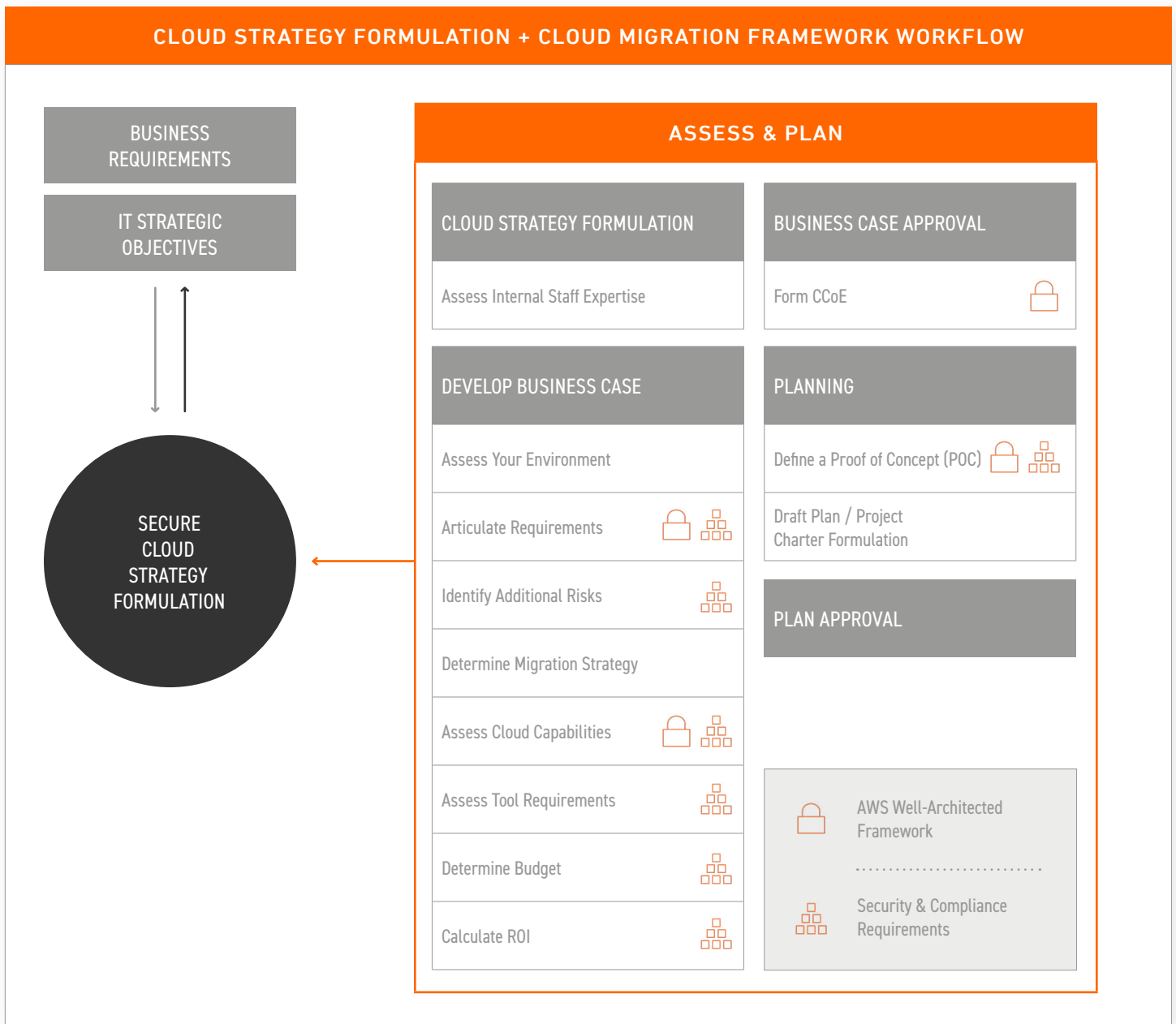
It will take the whole company to develop your cloud strategy:

- EXECUTIVE LEADERSHIP
- FINANCE
- HUMAN RESOURCES
- BUSINESS UNIT LEADERSHIP
- DEVELOPMENT/ENGINEERING
- OPERATIONS
- SALES
- MARKETING
- IT
- SECURITY
- GRC
- OTHER

## SECURE CLOUD MIGRATION FRAMEWORK



# HOW YOUR CLOUD STRATEGY FORMULATION + CLOUD MIGRATION FRAMEWORKS GO HAND IN HAND



## TRANSFORMATIVE THINKING & CONSULTATION

This stage is where all of your due diligence is advantageous to identify innovative opportunities to support the business and IT by leveraging the cloud. Because of the evolving capabilities of the public cloud, you may want to consider using an outside expert to help you ideate and strategize how to leverage the cloud to drive impactful and measurable results for your organization. Those results may be centered around supporting digital innovation, enhancing market agility, improving the customer experience, or a combination of reasons.

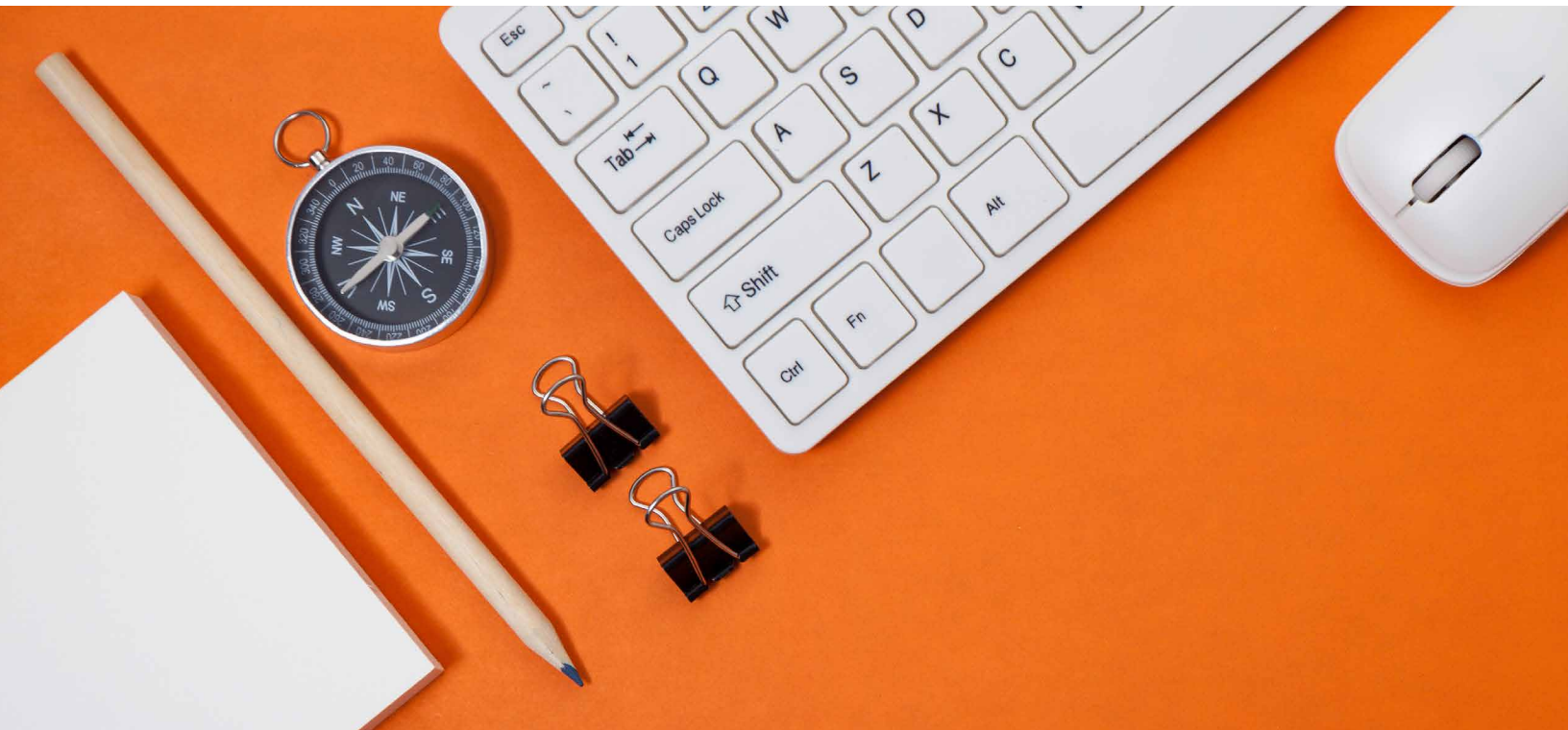
In addition, spend considerable time thinking through how security and compliance across this expansion of the IT estate may be re-architected and managed. New cloud native and third-party tools and technologies provide an opportunity for organizations to reengineer security and compliance in the cloud, which can then be extended to unify other parts of your hybrid environment. The graphic on the next page provides a list of security and compliance areas to consider as part of your transformation and modernization discussions.

### Transformation vs. Modernization

Although some may use the terms synonymously, we make a distinction between them.

We use *transformation* to indicate projects or initiatives that help transform operations for the business overall. The projects are a combination of technology, process, organizational change, and change management. *Modernization* refers more directly to the underlying technology or technologies involved and specifically how IT does business.

It's important to be very deliberate on what transformation means in respect to scope, deliverables, and metrics to determine overall success. In fact, we suggest that all transformation initiatives be broken down into very clear and actionable sub-projects or sub-initiatives as well as associated representative timelines.





## POLICY

- Shared Responsibility
- Articulation of Global Security and Compliance Policy for Cloud and Hybrid Environments
- Continuous Compliance
- Cloud-Agnosticism
- Multi-Cloud
- Proactive, Not Reactive
- Security and Compliance Early in the CI/CD Cycle

## TECHNOLOGY

- Cloud Native Security Toolsets and Services
- Automated Policy Automation and Adherence
- Automated Operations Efficiencies
- Workload Security
- Container Security
- IAM
- Logging
- Encryption
- Multi-Factor Authentication
- Segmentation
- Response in the Cloud

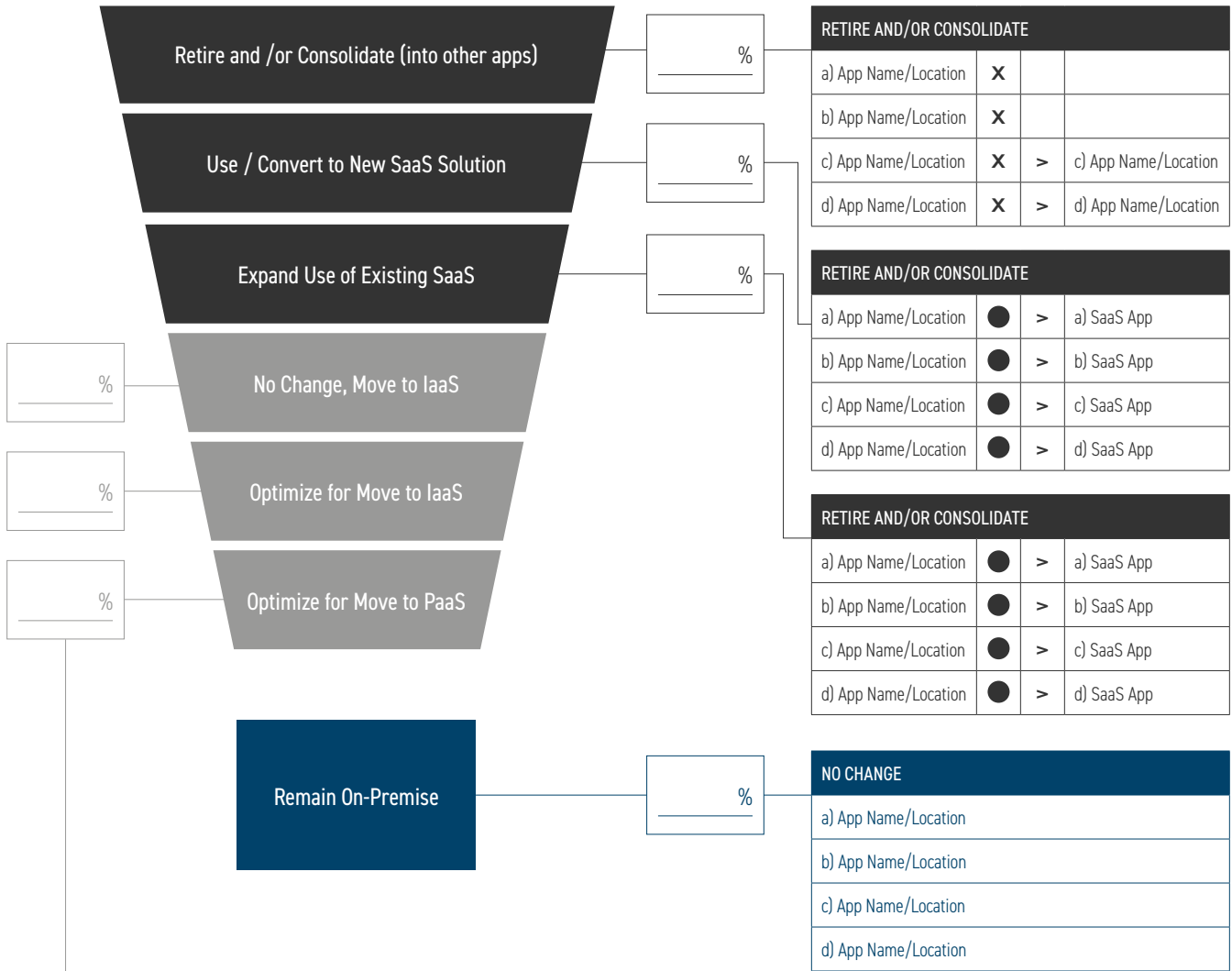
## ENVIRONMENT

- Containers
- Microservices
- Serverless
- Hybrid Environments
- Immutability
- Software-Defined Network
- Zero Trust

**Business transformation enabled by the cloud should also encompass transformation or modernization of your security and compliance program to gain similar scale, performance, and efficiency advantages.**

— Josh Bosquez, CTO,  
Armor

APP MIGRATION EVALUATION & PRIORITY WORKSHEET



GROUP 1		GROUP 2		GROUP 3	
a) App Name/Location	●	a) App Name/Location	●	a) App Name/Location	●
b) App Name/Location	●	b) App Name/Location	●	b) App Name/Location	●
c) App Name/Location	●	c) App Name/Location	●	c) App Name/Location	●
d) App Name/Location	●	d) App Name/Location	●	d) App Name/Location	●

**GARTNER'S 5 R's:** ● Rehost (Lift & Shift)   ● Refactor   ● Revise   ● Rebuild   ● Replace

Based on version Microsoft Enterprise Cloud Strategy White Paper, 2017.

## BUSINESS CASE/ROI DEVELOPMENT

Once you've identified opportunities and projects to support the business' and IT's overall objectives, it's now necessary to evaluate and prioritize the best ones. You may want to judge each initiative by criteria, including impact to the business, complexity, time-to-value, performance improvement, resources required, and cost, etc. You'll also want to consider the security and compliance implications for each initiative as

well as other risks. Be aware that your criteria may be more exhaustive than what your ROI analysis covers. Once you've put together your business case, it is then critical to get sign-off across your stakeholders and other vested parties. This should be a formality at this point as you should be openly working with and communicating to stakeholders throughout the entire process.

## SECURE CLOUD STRATEGY

Your approved business case effectively becomes your secure cloud strategy. At this point, execution is paramount. As we covered earlier and as you've seen by now, choosing a proven cloud migration framework is necessary to help you devise your cloud strategy in the first place. From this point on, the cloud migration framework is also what should guide the execution of your overall plan.



## PLAN COMPONENTS

### 1. SECURE CLOUD STRATEGY – EXECUTIVE SUMMARY

### 5. TECHNICAL TEAM RESOURCES

### 9. CLOUD MIGRATION

- Cloud Migration Framework
- Cloud Migration Assessment and Plan

### 13. RISK

- Risk of Failure to Business
- Risk to Success of Cloud Strategy Objectives
- Risk within Individual Key Initiatives

### 2. BUSINESS CASE OVERVIEW

### 6. ALIGNMENT OF OBJECTS

- Cloud Strategy Objectives Aligned to Business and IT Strategic Objectives

### 10. FINANCIAL & OPERATIONAL METRICS

- Overall ROI
- Metrics for Individual Objectives

### 14. CYBERSECURITY

- Global Policies
- Cloud Security (and Hybrid)
- Compliance
- Security and CI/CD
- Staff Training & Resources

### 3. DUE DILIGENCE

### 7. ROADMAP

- 12-to-18-Month Roadmap

### 11. CURRENT IT ENVIRONMENT

- Environmental Mapping
- Application Assessment and Prioritization

### 15. VENDOR PERFORMANCE

- Vendor Management
- Risk Management
- Risk Posed by Customers

### 4. VESTED PARTIES

### 8. CLOUD POLICY

- Global Cloud Policies
- Identification of Approved Platforms and Use Cases

### 12. PLAN FOR RETIREMENT

- Risk of Failure to Business
- Decommission Targets and Plan

# 11 CONSIDERATIONS BEFORE STARTING A MIGRATION PROJECT

Before you embark on your cloud migration project and overall journey to the cloud, it's critical to understand and consider a number of strategic areas first. These areas should influence your organization's thinking and planning regarding what drives your organization to the cloud and how you secure the applications and data that reside there.

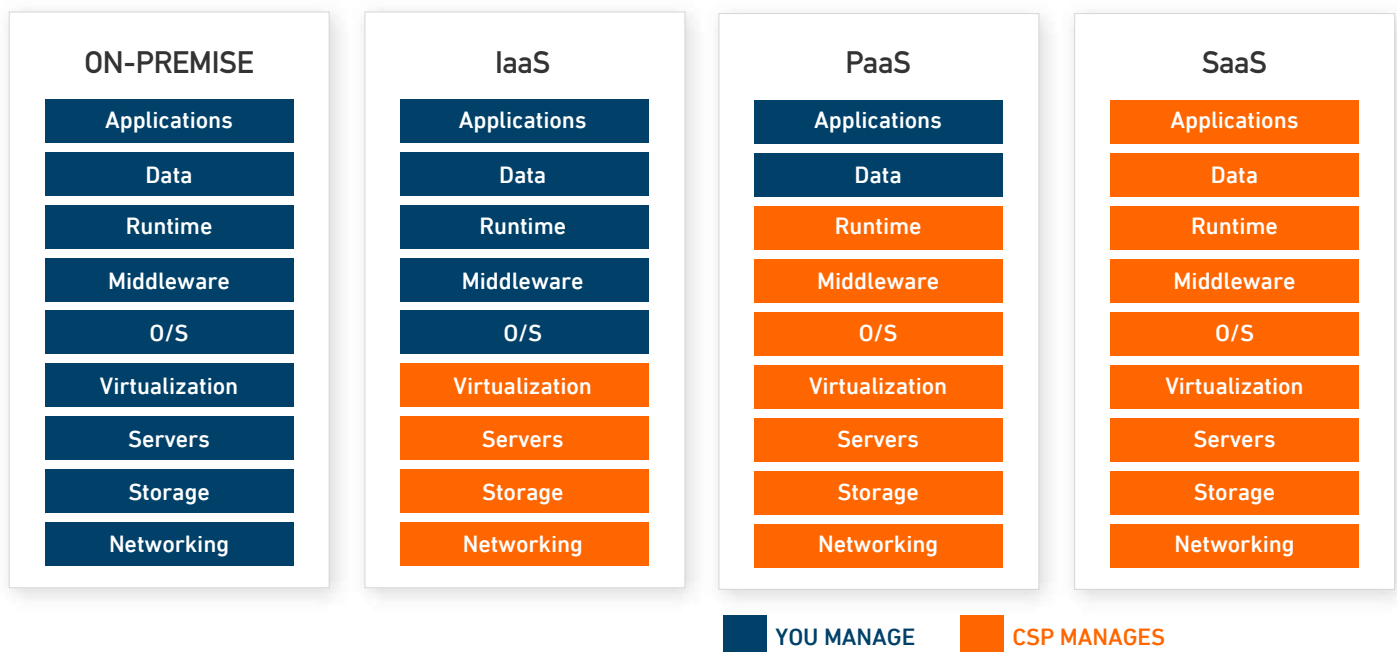
There is no order to the areas identified here as each may hold different weight based on the particular plans and needs of each organization.

## 1. SHARED RESPONSIBILITY

In the cloud, Shared Responsibility is black and white. The various cloud service providers go out of their way to make it clear where their responsibility ends and yours begins.

Before embarking on your cloud migration journey, make sure you know exactly what your organization is on the hook for across private cloud, IaaS, PaaS, and SaaS cloud-computing models.

Shared Responsibility is a key tenet for any cloud or hosted solution. And the level of responsibility the customer owns varies based on the different cloud platform types as depicted here. IT, Security, and DevOps teams need to have a keen understanding of shared responsibility for each cloud or hosted solution employed.



## 2. DEFINE YOUR MIGRATION GOALS

Are you looking to achieve great speed in your IT operations? Do you want to be able to respond more nimbly to changes in technological capabilities? Is your main goal improving the customer experience—or enhancing internal efficiencies?

Understanding what you want out of your cloud migration is the first step toward realizing it.

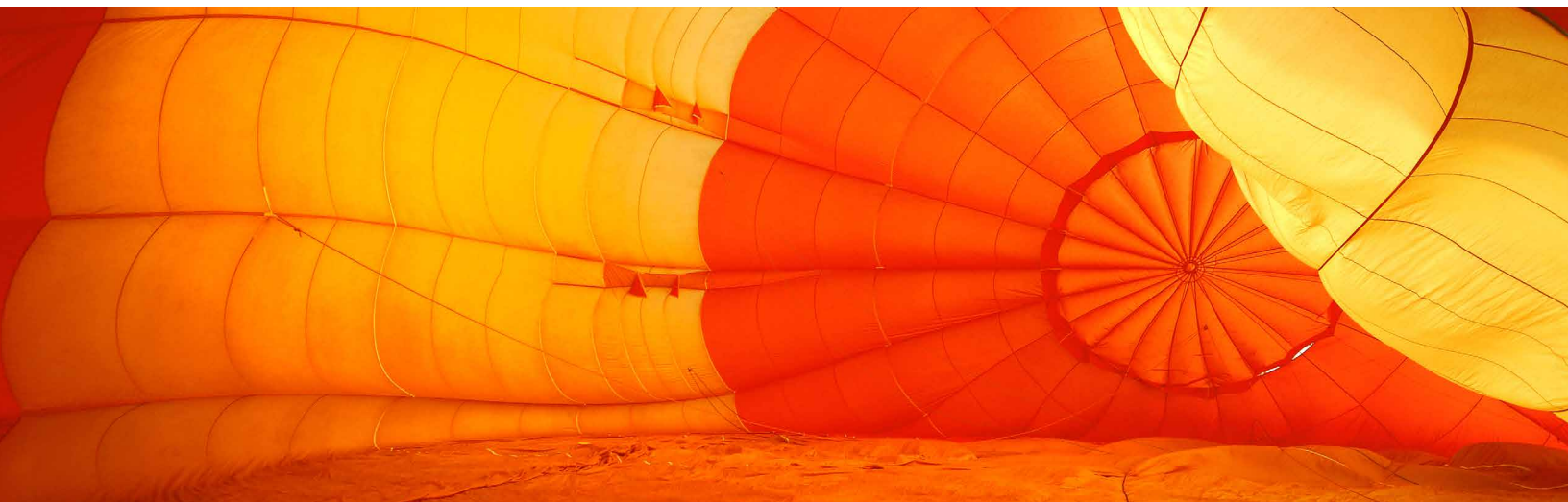
There are many great resources you can use to articulate and justify why your organization should migrate applications to the cloud. However, “getting to the cloud” isn’t the overall objective. Instead, there are usually key business and technical drivers powering consideration of the cloud as an enabler. And we’d make the argument that achieving rapid digital innovation in the future will rely on the cloud as the all-important enabling platform.

## 3. TRANSITIONING TO A SOFTWARE-DEFINED SECURITY MODEL

Migrating applications to the cloud represents a fundamental shift in how security and compliance are done versus in the past. We’re talking about moving to a model where everything is software-based. There is no hardware, and security is no longer defined by the perimeter.

The cloud represents an entirely different security and compliance paradigm. The faster Security and DevOps teams go from a focus on traditional on-premise and appliance-driven security and compliance practices to incorporate new skill sets and experience in securing cloud-based workloads, the better positioned they will be to help the organization accelerate the pace of innovation securely.

Security and DevOps teams need to honestly evaluate their cloud expertise, put plans in place to address gaps, and develop a solid cloud security competency across their staff. In fact, enterprises are already making this shift with 66% reporting they have a central cloud team in place, according to the RightScale 2019 State of the Cloud Report™. That figure drops substantially to 31% of SMBs having a central cloud team in place.



## 4. VENDOR LOCK-IN

Whether it's a standard policy not to be over-reliant on one vendor, or a corporate directive on high, you will need to consider the extent to which you are comfortable with using a single public cloud provider platform and how much you are willing to lock in your investment in that one platform.

With constant concerns for disruptors entering the marketplace, many organizations may employ a cloud-agnostic strategy to prevent enabling a potential competitor. Others may see a cloud-agnostic approach simply as an effective risk mitigation strategy. Identify whether your organization is likely to have concerns for over-investment in a single cloud platform and, if so, plan accordingly to address it.

## 5. MULTI-CLOUD IS BOTH A STRATEGY AND A NATURAL OUTCOME

Like a cloud-agnostic policy, pursuing a multi-cloud strategy can come as a choice by leadership or as a natural result of the analysis to determine what cloud environment best suits the specific requirements for each of the applications you are looking to deploy.

Whether it's a cloud-agnostic policy driving adoption or the findings of analysis that determine different applications have individual requirements best suited by different platforms, you may find your organization on the path to a multi-cloud strategy or policy. We argue that this outcome is inevitable for most organizations. Get ahead of whether your organization will pursue a multi-cloud approach and even outline what your organization's approach is now and potentially in the future.



## 6. ACCIDENTAL AND INTENTIONAL RISK

Because of the lower level of familiarity and experience with public cloud platforms, it's best to think of the cyber risk your organization can be exposed to. It could be "Accidental" cyber risk, or the risk introduced by misconfigurations, improper settings, and the honest mistakes (and not so honest) that can expose applications and data in the cloud. It could also be "Intentional" cyber risk, the risk introduced by threat actors targeting your application and data.

As organizations increasingly embrace the cloud, they must address both "accidental" and "intentional" cyber risk as part of their shared responsibility for security in the cloud. Cyber risk can be simplified down to the accidental risk introduced from things such as cloud misconfigurations and open settings and what IT or developers might do, to the intentional risk caused by bad actors targeting your company or ransomware encrypting your data.

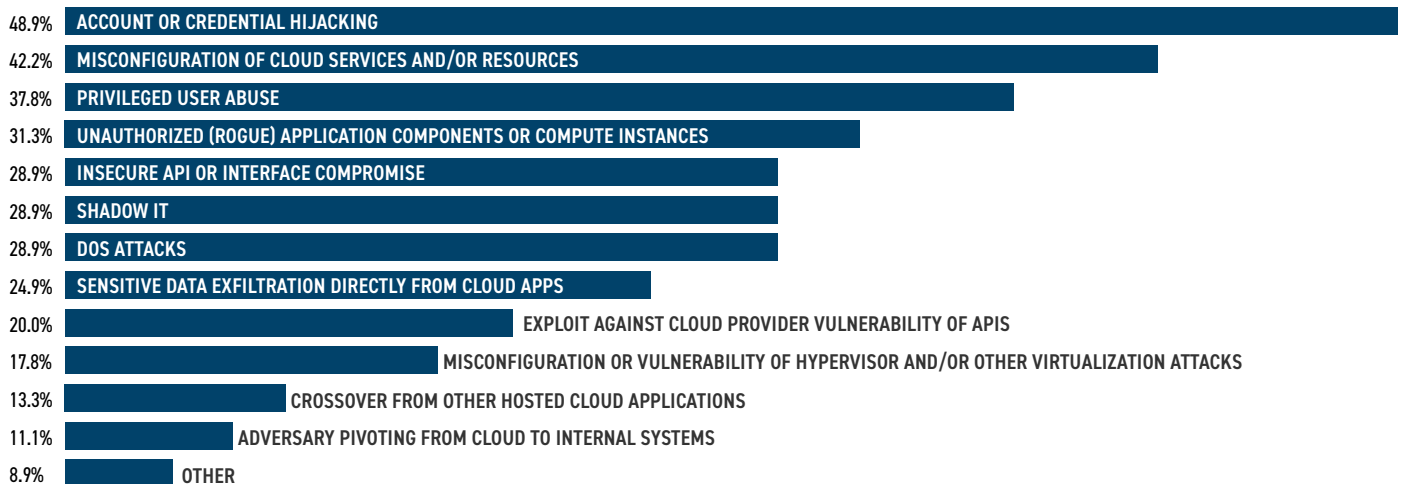
Fortunately, emerging technologies and capabilities such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) provide innovative approaches to address both areas of cyber risk while automating security and compliance processes.

Cloud Workload Protection provides multi-layer defense-in-depth protection for your workloads from intentional threats, helping you meet the requirements of your portion of the Shared Responsibility model. Typical solutions integrate host intrusion detection systems (HIDS), Malware Protection, File Integrity Monitoring, and Vulnerability Scanning and may include expert monitoring 24/7/365 as well as some degree of integrated incident response. These solutions can also be deployed across cloud, on-premise, and hybrid environments for unified visibility.

Cloud Security Posture Management technologies help you continuously discover, assess, and remediate security and compliance controls across your environment in the cloud. This includes identification of cloud misconfigurations and improper settings as a result of honest mistakes and negligence that could put your applications and data at risk of exposure. In addition, CSPM solutions can provide an opportunity for organizations to establish a global security policy for assessing and managing risk across their cloud environments.

The combination of the two solutions, in concert with other security protections, represents a powerful opportunity to elevate the security and compliance posture for your cloud environment.

### TYPES OF INTENTIONAL ATTACK THREAT VECTORS





## 7. REACTIVE VS. PROACTIVE

Traditional security operations in the on-premise world are largely reactive in nature, reacting to the first sign of a threat hitting the perimeter or the first missed checkbox on a compliance audit. The cloud changes everything.

With new capabilities such as CSPM, CWP, and native tools being rolled out regularly, IT, Security and DevOps teams can put security on a proactive footing while automating and simplifying operations in the process.

It's important to recognize this opportunity to drive a stronger security posture while capturing efficiencies at the same time. Make sure you engage your IT, Security, and DevOps teams responsible for application and data security on this and other topics in this paper—thus providing time to consider and capitalize on the opportunities the cloud presents in redefining the active nature of your security and compliance operations.

### Accidental Cyber Risk

Over a 2-year period, 920 million records were inadvertently exposed publicly as a result of an AWS S3 misconfiguration. Of the incidents identified, 8 involved data exposed by an affiliate, partner, or customer of a larger organization.

Unintentional, insider-originated security breaches can be the result of simple negligence, inattention, or lack of awareness or training. Unintentional mistakes such as system administrator errors, operator errors, and programming errors, are common.



## 8. SECURITY EARLIER IN THE DEVOPS CYCLE

DevOps practitioners must be able to drive secure code development and deployment with as little friction and complexity as possible along the way. And anything that gets in the way of delivering more code in support of business objectives typically means serious trade-offs.

However, security and compliance practices integrated early into the DevOps cycle and automated to enhance the overall protections afforded to your applications is entirely possible in the cloud.

Pressure to accelerate the pace of business puts demands on the teams involved in supporting business initiatives and innovation. That places pressure on Development and IT teams responsible for pushing out new code and supporting those initiatives and innovation. Security and compliance functions must line up to the new reality that controls are deployable at the speed of development with as little resistance as possible.

By integrating security and compliance controls early into the DevOps process, IT, Security, and DevOps teams can match the pace of development. In addition, new capabilities can act as guide rails for best security and compliance practices for developers through their coding efforts.

Last, this approach begins to put the goal of immutability within reach.

## 9. IMMUTABILITY

Imagine the future where security protections are enhanced by a constant ebb and flow of your instances being wiped and recreated daily or even hourly. This makes it even harder for an advanced threat actor to establish a foothold in your environment and have the time to cause any actual harm.

IT, Security, and DevOps teams need to think now about the pieces they can put in place to move toward immutable infrastructure and workloads. As cloud security experts, we see a lot of promise in adopting this kind of regimen. Security and compliance protections are integrated early into the DevOps cycle, and workloads are unchangeable once they are put in production—thus increasing the difficulty for threat actors to gain and maintain a secure position in your cloud environment.

Additional benefits of immutability include:

- Eliminates disruption to product applications for patching and updates as these are done on the gold image and then rolled out.
- Reduces risk of disruption or downtime associated with testing as testing is performed on the gold image.
- Accelerates roll-out of application updates.
- Easily detects unauthorized changes to production applications (combined with security capabilities such as File Integrity Monitoring), resulting in automated deletion and regeneration of the application.

As organizations consider the advantages of immutable infrastructure, they should consider the business and technical advantages of containers as one aspect of this infrastructure.

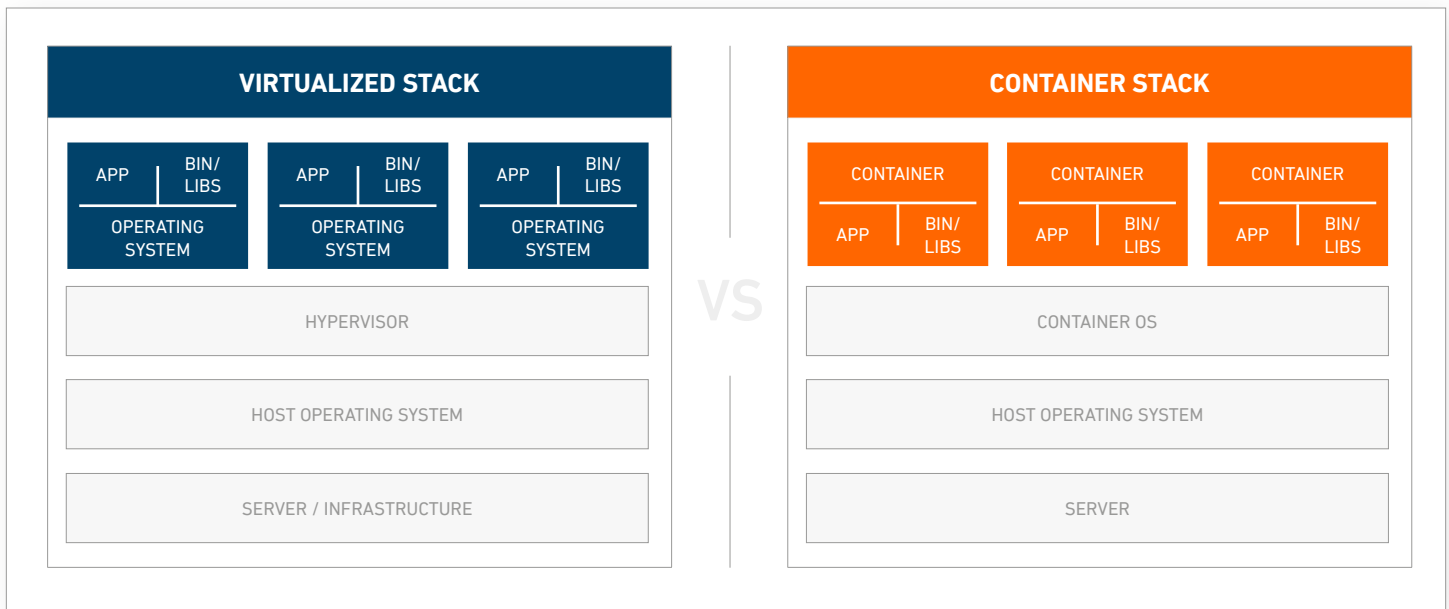
## 10. ANTICIPATING OPPORTUNITY

Containers, serverless, and microservices architecture present tremendous benefits for organizations—ease of deployment, portability, scalability, and the ability to act as a hedge against vendor lock-in.

As you plan your migration, you will want to future-proof your planning to provide allowances for container usage and serverless deployments, as well as identify any applications where a microservices architecture will make sense (not for every organization or for just any application).

Containers are as they sound—they hold something. In this context, a container is a logical storage box that houses an application and its related components. The concept of containers is not new, though their usage has accelerated with the increased adoption of the cloud. Docker, a computer program that “virtualizes” (i.e., containerizes) operating systems (OS), refers to containers as simply, “a standardized unit of software.” Forrester offers a more specific description: “Containers bundle applications with the software libraries that they depend on, allowing developers to create ‘build once, run anywhere’ code, making applications very portable.”

DevOps and development teams are the primary force driving the adoption of containers because of the accelerated time-to-market for deployment of testing and production environments for new applications. Meanwhile, IT may be pushing the use of containers to move legacy applications into the cloud with the intent to refactor some of those applications in the future.



Though security teams may see the advantages inherent in the use of containers, it's unlikely they would push container usage unilaterally—especially without clear security solutions in place to protect them. But development and DevOps already see the value of containers and leverage them. Smart security teams would likely want to exploit their full security value in the future.

■ **PRODUCTION DEPLOYMENTS**

According to 451 Research, 52% of enterprises are either in the initial stages or have broadly deployed production applications in containers.

■ **MICROSERVICES DEPLOYMENT**

Containers are particularly ideal for microservices deployments, which break down traditionally monolithic or large-scale application architectures into specialized micro applications.

■ **DEPLOYMENT OF DEV APPLICATIONS FOR TESTING**

Containers allow for rapid deployment of applications under development and testing, eliminating the complications associated with configuring and managing the underlying host OS. The ability to spin containers up and down quickly and easily aligns with the needs of DevOps and developer teams.

■ **'LIFT & SHIFT' OF LEGACY APPLICATIONS**

Whether refactored or not, deploying legacy applications in containers can accelerate the shift to the cloud, while freeing up an enterprise's costly on-premise resources and footprint.

■ **RUNNING OF TRIALS & PILOT PROJECTS**

Containers also provide an efficient mechanism to run trials and pilot projects without the additional overhead associated with managing the OS or infrastructure.

## 11. THE SOFTWARE-DEFINED NETWORK

Be sure to research and comprehend how a Software-Defined Network model based on Zero Trust and the use of micro-segmentation could enhance security across your presence in the cloud. Whether this is something your organization is ready for or not, be cognizant of how your organization could adopt such a model in the future.



[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

20010318 Copyright © 2020. Armor, Inc., All rights reserved.