How To Gain Control Of Your Microsoft Azure Environment

VAST
IT without Limits™

POWERED BY CloudHealth

INTRODUCTION

In today's fast-moving, competitive environment, companies are migrating to Microsoft Azure to increase their agility and decrease their time to market. While the payoff for adopting Azure can be great, many are finding it difficult to reach the cloud and business success they originally hoped for.

It's common for organizations investing in Azure to encounter numerous roadblocks early in their cloud journey, including monthly bills exponentially higher than anticipated and underutilized resources. For organizations looking to reach cloud maturity—where cost and performance are optimized, security and compliance best practices are established, and one's environment is governed by policy-driven automation—gaining control of their Azure infrastructure is crucial.

The goal of this eBook is to help with just that. For those of considering Azure or who are currently in the migration phase of your Azure cloud journey, we offer insight and expert best practices to make the early stages of your journey as smooth as possible. For organizations already using Azure services, we dive deep into improving cost management, resource optimization (including best practices for reducing cloud waste), and what governing your cloud ecosystem with established security standards and automated policies can look like.

WHY IT'S IMPORTANT TO GAIN CONTROL OF YOUR AZURE ENVIRONMENT

In 2018, Gartner predicted that by 2020, 30% of all data breaches will be attributable to Line of Business IT.[1]

[1] *Gartner, CISO Playbook: How to Retain the Right Kinds of Control in the Cloud, Steve Riley, 10 July 2018*

Before the cloud, most organizations operated on-premises data centers. With on-premises infrastructure, it's easier to project your upfront infrastructure costs, keep track of what assets you have, and know how your data is being secured. Once you start operating in Azure, it's a slippery slope to losing control over your cloud ecosystem. Compared to on-premises infrastructure, cloud infrastructure comes with a significant lack of visibility—and with it a lack of control. Regaining—and ultimately maintaining—visibility into your Azure ecosystem is essential to your continued success in the cloud.

Many organizations claim to have their cloud ecosystem under control, but cloud experts report Line of Business IT (or Shadow IT) is much more prevalent than CIOs believe. Not only does this create problems for keeping costs under control, but this lack of oversight also negatively affects asset performance and introduces numerous security risks.

BENEFITS TO INCREASED CONTROL

It's not just about the money. While the effort put into efficiently managing costs will be financially worthwhile, gaining visibility over all of your Azure infrastructure will allow you to optimize resources for better performance and proactively close security gaps.

Gaining control of your Azure environment also allows you to govern with confidence. This means having guardrails in place to standardize your business' cloud operations, which in turn gives you the ability to make well-informed, data-driven decisions and quickly respond to market changes—ultimately giving your business a competitive edge over market rivals.

WHERE ARE YOU IN YOUR AZURE JOURNEY?

Because every organization is at a different stage in their Azure cloud journey, we've divided our eBook into four sections:

1

STAGE 1: MIGRATION

It's important to know what to look for when comparing cloud service providers and ways you can make your migration as smooth a project as possible.

2

STAGE 2: COST MANAGEMENT

If you've been overspending month after month you're not alone—understanding Azure's pricing and discount models, as well as knowing a few key cost management tips can, help you reel back in your monthly Azure spend and get back on financial track.

3

STAGE 3: RESOURCE OPTIMIZATION

Properly monitoring the utilization and performance of your resources can help you further reduce cloud waste. Maintaining an efficient cloud ecosystem is an important step to scaling your cloud infrastructure.

4

STAGE 4: GOVERNANCE AND SECURITY

Governing your Azure environment through automated actions and established policies will streamline your organization's cloud processes and help enhance security, operations, and more.

VAST
IT without Limits™

1 MIGRATING TO AZURE

WHY BUSINESSES MOVE TO THE CLOUD

Different businesses move to Microsoft Azure for different reasons. Among the most common reasons are to take advantage of increased availability, flexibility, and scalability, and to replace aging on-premises legacy systems with more productive cloud-based systems. Cost is also a major factor, as operating in the cloud with proper cost management can save businesses a considerable amount of money.

Migrating all or part of your on-premises infrastructure to Azure is no easy task. Without the proper people, processes, and technology in place, migrations can easily run over-budget or behind schedule. The key to migrating to Azure successfully is to do so when the time is right, and only with assets and applications that need to be migrated to the cloud.

An increasing number of businesses are migrating to Microsoft Azure because of its extensive services portfolio and investment in emerging and open source technologies. Microsoft is also continuing to open more regions to address data compliance requirements, which has the additional benefit of reducing latency.

BEST PRACTICES FOR A SMOOTH MIGRATION TO AZURE

If Microsoft Azure ticks all the right boxes for your organization, the first stage of migration is to conduct a cloud migration assessment.

A migration assessment should include:

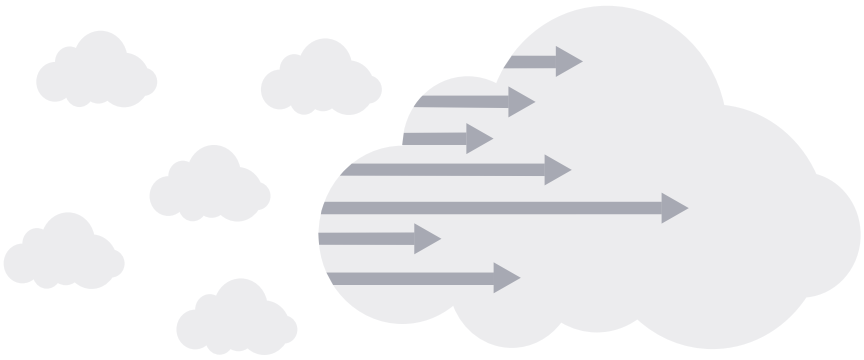
- Identifying workloads in your existing infrastructure that are suitable for migration to the Azure Cloud
- Using this information to decide on a migration strategy
- Calculating the Total Cost of Ownership (TCO) to determine your costs compared to the benefits of moving to the cloud

MIGRATING TO AZURE

Developing a cloud migration strategy helps define your motivations and goals for adopting the cloud, and ensures your roadmap will get you there in the end. Businesses' motivations for adopting the cloud typically include reducing IT spend, improving IT efficiency, gaining access to new technologies, having the capability to expand quickly, and enhancing their security posture.

Once you've defined your business' motivations, the next step is to determine which assets to migrate and how you'll go about migrating them. You may decide to initially transition only some of your existing workloads, or refactor some workloads not currently compatible with Azure. Alternatives include refactoring all your existing infrastructure, or a "lift-and-shift" migration, in which you rehost legacy systems on the new platform.

As cloud migration strategies evolve it's important to be aware of the TCO when strategies change. TCO is effectively a comparison of thedirect and indirect costs of moving to the cloud weighed against the direct and indirect benefits, such as freeing up the time and resources of your organization's internal IT team to focus on more strategic initiatives.



2 COST MANAGEMENT

WHY YOU'RE OVERSPENDING IN THE CLOUD

Regardless of how well you plan your cloud migration strategy and calculate your Total Cost of Ownership, you're likely to spend more than necessary when you first migrate to the cloud. Don't worry, you aren't alone. In 2018 Gartner forecasted: "Through 2020, 80% of businesses will overshoot their cloud IaaS budgets due to a lack of cost optimization approaches". Gartner attributed the failure to manage cloud costs to three key challenges businesses are struggling to overcome:

- Complex multicloud environments in which different Cloud Service Providers provide "dramatically different" billing details.
- Central IT departments who were used to on-premises infrastructures, and who now lack the processes to manage costs in the cloud.
- A failure by IT departments to consider the business' overall cloud strategy, and instead focusing on "getting the job done".

It's also the case that Virtual Machines (VMs) are usually more efficient and work faster than their on-premises equivalents. Consequently, developers often configure resources with like-for-like attributes rather than calculating the actual CPU, memory, and bandwidth required for VMs to do the same job in the cloud. When the deployment works successfully, the configuration then becomes a template for subsequent deployments—replicating at over-capacity and increasing costs unnecessarily.

One common misconception is that you only pay for what you use when you deploy resources in the cloud. In reality, you actually pay for what you provision. So, if you provision an Azure D8s v3 VM with 8 vCPUs, 32 GiB of memory, and 64 GiB of temporary storage, that's what you'll pay for whether you use the VM's full capacity or not. You'll also continue to pay for the VM when it's idle, so remember to always switch them off when you've finished using them!

BEST PRACTICES FOR KEEPING CLOUD COSTS UNDER CONTROL

Best practices for keeping cloud costs under control may differ from business to business depending on whether a partner is being used (who will implement the best practices for you), whether the business has an existing Enterprise Agreement, and the nature of resources being deployed.

For most businesses, these three best practices apply:

- **Gain visibility into your cloud spend.**
  It's important to know what resources are being used, by whom, and for what. Driving accountability to specific teams or project owner can ensure responsible cloud usage moving forward and will help finance understand and track costs for future budgeting.

- **Monitor the burndown of your EA.**
  You may be able to get a better discount by committing to more usage, but don't overcommit yourself. While the discounts may seem enticing, they will only save you money if you actually need the resources. Buying something just because it's on sale doesn't actually save you money if you never end up using it.

- **Purchase Azure Reservations to reduce costs.**
  These can be cancelled or exchanged if your circumstances change, so don't be afraid to investigate the practicality of these discount options out of fear of a multi-year commitment. Just be sure to rightsize your assets before you buy reservations for optimum cost savings.

VAST
IT without Limits™

3 RESOURCE OPTIMIZATION

PICKING THE RIGHT CLOUD INFRASTRUCTURE TO SUPPORT YOUR WORKLOADS

Optimizing your resources involves provisioning the right resources—and the right size of resources—to support your workloads at the best possible cost.

Provisioning resources correctly can be difficult if you're still operating with an on-premises mindset because there is a greater range of products and services available for use in the Azure Cloud that might be new or unfamiliar. For example, optimally using your cloud environment could involve using containers, burstable VMs, and Load Balancers instead of general use VMs. In order to find the right balance, you need to understand what products and services are available, as well as continue to monitor the resources you've already deployed. Monitoring will help you assess the utilization and performance of existing resources to determine whether the workloads running on them would be better suited for a different type of product or service.

WHY YOU SHOULD CONTINUE MONITORING UTILIZATION AND PERFORMANCE

Azure provides a range of native tools to help businesses monitor the utilization and performance of resources that work well if you have a limited number of deployments. However, as you expand your Azure services portfolio, it's beneficial to invest in a third-party cloud management solution that can accumulate utilization and performance data from all sources and all clouds into a single dashboard.

Resource optimization is not a one-time task. Many teams accurately provision resources when they first migrate to Azure, and then stop because they believe the job is done. In reality, you should be monitoring utilization and performance at all times to maintain an optimized cloud ecosystem, as the demand on resources can change over time.

This may sound like time-consuming work, but monitoring tools can be configured to alert you to changes in resource demand you so can upgrade or downgrade assets when necessary to reduce costs. The key metrics you need to keep an eye on (or configure the monitoring tool to keep an eye on) include CPU, memory consumption, disc space, network usage, and throughout.

BEST PRACTICES TO FURTHER REDUCE CLOUD WASTE

Cloud waste manifests in many forms aside from just over-provisioned resources. And although rightsizing will contribute towards managing costs and optimizing resources, there is more you can do to minimize cloud waste—or eliminate it all together.

These best practices can help you identify where your money is being wasted in the cloud:

DELETE UNATTACHED DISK STORAGE

DELETE AGED SNAPSHOTS

TERMINATE ZOMBIE ASSETS

UPGRADE RESOURCES TO THE LATEST GENERATION

SCHEDULE START/STOP TIMES FOR NON-PRODUCTION RESOURCES

VAST
IT without Limits™

DELETE UNATTACHED DISK STORAGE

When a VM is launched, Disk Storage is automatically attached to act as the local block storage. When you terminate the VM, its Disk Storage remains active unless you terminate it manually. By checking for unattached Disk Storage in your Azure environment, you can cut thousands of dollars from your Azure bill.

MOVE OBJECT DATA TO LOWER-COST TIERS

Microsoft Azure offers several different classes of data storage depending on how frequently the data is accessed and the level of accessibility (redundancy) required.If you have object data which is not frequently accessed and not required to be safeguarded for compliance purposes, you should move it from a Hot storage tier toa lower-cost, Cold storage tier.

DELETE AGED SNAPSHOTS

Many businesses use Snapshots to create point-in-time recovery points in case of data loss or disaster. However, in the event that you need to use a Snapshot, you're only ever going to need to use the most recent version available. Closely monitor what Snapshots exist in your Azure environment and delete them once they are no longer required or out of date.

TERMINATE ZOMBIE ASSETS

Aged Snapshots may not only be the only resources in your Azure environment incurring unnecessary costs. Other zombie assets to look out for include resources attached to the failed launch of a VM, idle Load Balancers, idle SQL Databases, and unused IP addresses. Microsoft will charge for these resources for the time they are running.

UPGRADE RESOURCES TO THE LATEST GENERATION

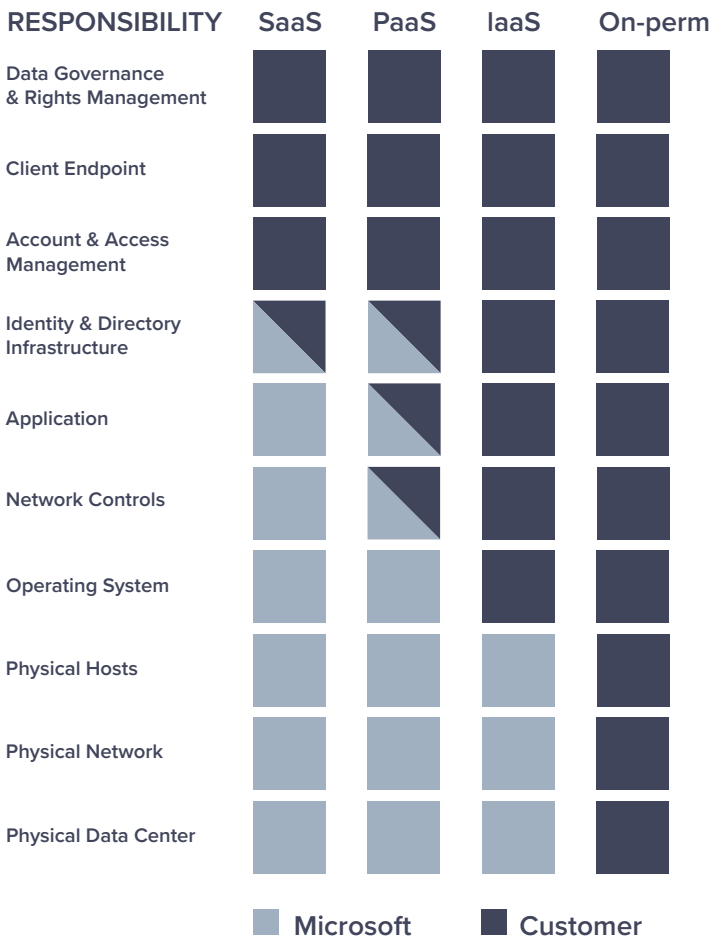
Microsoft often upgrades elements of its Azure portfolio with improved capabilities and additional functionality. A good example of this is when Azure "Classic" VMs were upgraded to Azure "Resource Manager" VMs in 2014, which gave businesses up to 35% faster processing speeds and greater scalability for the same price point.

SCHEDULE START/STOP TIMES FOR NON-PRODUCTION RESOURCES

Most of the resources you deploy on Azure will be used around-the-clock, but not all. These non-production resources should have start/stop times scheduled to reduce costs. For example, if you schedule VMs used for development to only be running between 9.00 a.m. and 5.00 p.m. Monday to Friday, you will save 76% of the cost of running them.

4 GOVERNANCE AND SECURITY

A certain amount of responsibility is owned by Microsoft depending on the services you use. The distribution of responsibilities for Azure Cloud is illustrated below:



What you should focus on when developing your Azure management strategy is how to gain control of the Azure infrastructure and environment you have responsibility for. Gartner provides a rather good analogy to help explain this concept, in which taking a journey by car (on-premises) is compared to taking a journey by plane (cloud).

On the car journey, you're in control of the vehicle. You're also responsible for filling it with gas, checking the oil, and maintaining the tires. On the plane journey, these responsibilities are taken away from you and managed by the airline. You still have the responsibilities of selecting your destination, arriving at the airport prepared to fly, and acting appropriately during the flight. And if you are able to meet your responsibilities, you'll enjoy a cheaper, quicker, and (statistically) safer journey than if you had chosen to drive. This is how you can think about Microsoft's responsibility model, where Microsoft assumes the responsibilities of the airline and you are responsible for showing up and traveling.

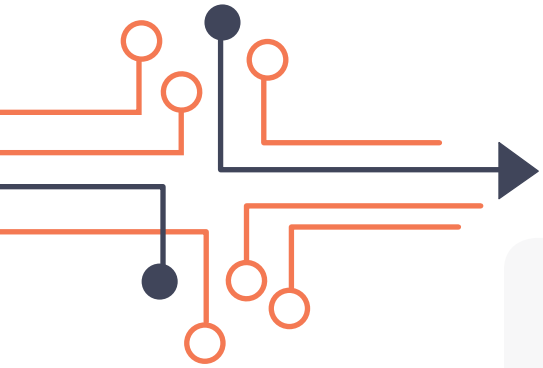
WHY YOU NEED GOVERNANCE

Governance in the cloud shouldn't be compared to governance in an on-premises environment. Although similarities exist with regard to rules, policies, and processes to monitor operations, in the self-provisioning environment of the cloud (where resources can be launched with a simple click of a mouse), rules, processes, and policies have to be built differently to keep cost managed, resources optimized, and data secure.

If you've implemented the best practices mentioned in previous sections, tighter control of operational policies should help you maintain control of your Azure environment. Once governing policies are in place you'll be able to make well-informed, data-driven decisions, quickly respond to market changes, and focus on driving value to your business instead of managing back-end infrastructure.

OPTIMIZING COST AND PERFORMANCE WITH AUTOMATION

Automating governance in the cloud consists of first identifying simple or repetitive tasks, and then configuring automation software with policies that apply to those tasks. Automation software monitors your Azure environment around the clock, and takes user-defined actions when anomalies occur that violate your policies.



Cloud governance policies fall into six categories:

- Financial Management
- Operational Governance
- Asset and Configuration Management
- Cost Management
- Performance Optimization
- Security and Incident Management

FINANCIAL MANAGEMENT

If the projected month-to-date spend is greater than 100% of budget, send an email notification to the budget owner.

OPERATIONAL GOVERNANCE

If a snapshot is older than 2 months and subsequent snapshots exist, delete the older snapshot and send an email notification to the owner.

ASSET AND CONFIGURATION MANAGEMENT

If an asset is launched lacking a tag or with a tag that does not conform to your tagging policy, stop the asset and send an email notification to the owner.

COST MANAGEMENT

If an Azure Reservation is utilized less than 60% during the month, send an email notification for possible exchange or cancellation.

PERFORMANCE OPTIMIZATION

If the average CPU usage of a Virtual Machine OR memory usage OR disk throughput OR network throughput exceeds 80%, send an email notification for a potential upgrade.

TAKING ADVANTAGE OF AUTOMATION TO ENHANCE CLOUD SECURITY

Microsoft remains responsible for certain elements of Azure security. In the case of IaaS services, these responsibilities extend to the physical data center, the physical network, and the physical hosts. Everything else related to security is your responsibility, including such things as who has access to your account, how your virtual cloud environment is secured, and what precautions are taken against a data loss or disaster.

Generally-accepted best practices for security in the cloud include implementing role-based access controls with least possible privilege, defining the guardrails under which the business operates in the cloud (the rules, policies, and processes of cloud governance), and validating your security posture against industry standards. However, these are only effective best practices when the means exist to enforce them. This is where automation can enhance your cloud security.

In the same way as automation software can manage and optimize costs and performance, it can also be used to enhance cloud security by monitoring simple and repetitive activities in your cloud environment and alerting you to anomalies, or by taking a user-defined action when a security policy violation occurs.

Example policies for enhancing security in your cloud environment include:

- If an IAM user has multi-factor authentication disabled, revoke the user's access and send an email notification to the user.
- If a VM has unauthorized open ports, terminate the VM and send an email notification to the owner.
- If an unusual volume of resources is launched outside normal usage patterns, stop resources and start workflow approval process.
- If an IAM user logs into the account from an unrecognized IP address, revoke the user's access and send an email notification to an administrator.
- If an Azure storage volume is publicly accessible, restrict access to the volume, encrypt its content, and send an email notification.

WHERE DO YOU GO FROM HERE?

Whether you're approaching Azure for the first time, or are an Azure veteran, gaining control of your Azure environment is pivotal for obtaining maximum benefit. Here are a few next steps to help you can regain and maintain control of your Azure investment.

- Having control of a cloud environment is different than having control of an on-premises environment. Learn more about Azure's shared responsibility model to ensure you understand where Microsoft's accountability ends, and where yours begins.

- The cost of a bad migration to the cloud far outweighs the cost of a good migration, so take time to start planning your migration strategy with key stakeholders. A good place to start is identifying which workloads are best suited for migration.

- There is a misconception that you only pay for what you use when you deploy resources in the cloud. What you actually pay for is what resources are provisioned, so make sure you're taking advantage of easy rightsizing opportunities to quickly optimize resources and cut costs.

- Resource optimization is not a one-time task. You should be monitoring utilization and performance at all times. Choose a solution that monitors your environment for you and give your team hours back in the day to focus on projects that matter most to your business.

- In the cloud, there is a lot more governing to do than in an on-premises environment. Effective governance has its benefits, including anomaly detection and automated alerting.

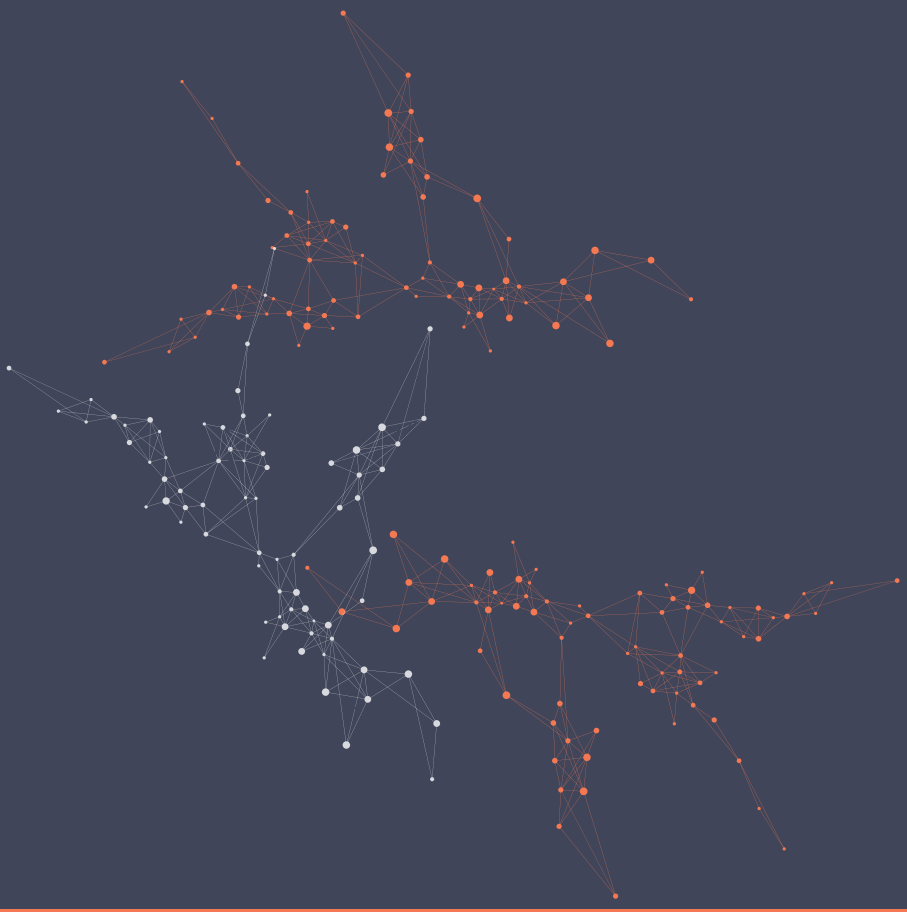
- Automation is nothing to shy away from. It enables you to do more with less. Start by identifying a handful of simple or repetitive tasks that are prime automation candidates and practice building policies that fit, such as deleting snapshots older than 2 months if subsequent snapshots exist.

CONCLUSION

It's important to remember that these best practices are not meant to be one-time activities, but ongoing processes. Because of the dynamic and ever changing nature of the cloud, cost optimization activities should ideally take place continuously.

Learn more about how you can help you automate the continuous optimization by visiting **www.vastITservices.com**

POWERED BY CloudHealth



VAST
IT without Limits™