Microsoft 365 Cloud Strategy Excellence

MYTH OR REALITY?

This eBook is a comprehensive guide on how to develop **a cloud-first strategy** in Microsoft 365. Learn tips & tricks and how to tackle common challenges!

SysKit

Contents

About the Author

Chris Hardee is a 20-year technology professional who found a passion for writing and marketing. He enjoys diving deep into technical concepts, finding important points in the data, and translating them into the right words. He's written for several major online publications, including Forbes, Business 2 Community, and MISTI Training Institute.

In his free time, Chris enjoys flying drones, going for walks with his two dogs, reading, and spending time with family.

Introduction

The cloud will grow by 21.1% in 2021, according to Gartner. By 2026, public cloud will account for over 45% of enterprise IT spending.

"The economic, organizational, and societal impact of the pandemic will continue to serve as a catalyst for digital innovation and adoption of cloud services. This is especially true for use cases such as collaboration, remote work, and new digital services to **support a hybrid workforce**," says Henrique Cecci, Gartner senior research director.

Many businesses will focus on cloud-first strategies like Microsoft cloud where companies move most of their infrastructure to the cloud to get a competitive advantage.

"If you have not developed a **cloud-first strategy** yet, you are likely to **fall behind your competitors**. IT organizations have moved past asking whether applications can be deployed or migrated to the public cloud. Instead, they are commonly **accepting that the pace and innovation of cloud providers** is foundational to their business," says Elias Khnaser, VP analyst at Gartner.

Many businesses will focus on cloud-first strategies like Microsoft cloud where companies move most of their infrastructure to the cloud to get a competitive advantage.

Rapidly approaching cloud trends

To prepare for this shift to the cloud, you need **a cloud-first strategy**. These trends listed below will help you prepare.

The rise of hybrid work

The pandemic has had a **substantial impact on the cloud**. In 2019, there were an estimated 365 million desktop computers used in offices around the world. After the pandemic started in 2020, almost **1 billion people switched to working from home**. This change leaves IT leaders with the challenge of finding the **best way to work with this hybrid working environment** where some employees work at home and in the office.

Computing at the edge

Typically, when you think of edge devices, you're referring to the Internet of Things (IoT). However, Microsoft has been **expanding its portfolio using edge devices**. Some of these include Azure Stack Edge Pro, and Pro R. Microsoft has announced that it incorporates all devices with **onboard AI processing capabilities** as its intelligent edge device. The Azure modular data centers are also edge devices.

Microsoft believes that edge is the **future of the cloud**. In 2021, business models will support the deployment of the edge along with AI and 5G. With this type of a centralized cloud system, serverless computing models will **slowly take over the industry**.

"And now we're taking cloud compute to the edge with 5G deployments. Our new Azure edge services help operators and enterprises **deliver ultra-low latency compute fabric**. And we're also helping operators run their networks in the cloud," says Microsoft CEO Satya Nadella.

IoT

The Internet of Things (IoT) has gained immense popularity in recent years for its ability to provide an **endless stream of data on customer behaviors**. That is, being able to tap into this wealth and use it how you see fit - whether by marketing your products more effectively or providing **better service at every touchpoint imaginable**. These benefits are primarily thanks to our world going fully remote during pandemic times.

Improved cloud management

Performance management and automated services are **essential factors you need to consider** when selecting a cloud computing platform. Many enterprises have moved entire workloads to the cloud to **achieve operational efficiency**, but their cost has also increased in the process. With Azure, you get a cost-effective solution and only pay for the services you use. This change will allow you to stop cloud wastage and improve cloud management.

With Azure, you get a cost-effective solution and only pay for the services you use. This change will allow you to stop cloud wastage and improve cloud management.

Machine learning and security

Machine learning is a crucial part of the cloud computing landscape. Microsoft Azure Machine Learning provides a user-friendly set of tools and algorithms that **provide accurate predictions**. It will allow you to **import training data and then fine-tune the results**.

Azure Machine Learning also helps protect the cloud. First, deep learning can **catch malware** while analyzing endpoints like servers and desktops, while machine learning plays a significant role in **threat intelligence**. Machine learning exists in behavioral-based solutions, which try to **identify malicious behavior** in monitored endpoints.

Machine learning is **revolutionizing cybersecurity software**, with companies using all kinds of artificial intelligence to better protect their customers.

Whether it's cybersecurity, IoT, or edge, challenges still exist for the cloud.

Challenges with the cloud

Many of the obstacles security leaders will face in 2021 will have to do with the unique challenges of the cloud.

1. Not enough cybersecurity investment
2. Knowledge gap in cybersecurity
3. Breakable permissions inheritance
4. Sharing files without a password
5. Microsoft 365 audit log is not real-time
6. Understaffed and overworked IT can mismanage servers and equipment

1 Not enough cybersecurity investment

A common assumption is that security teams will **effectively protect an organization** regardless of what management decides to do. The reality is cybersecurity teams **don't have big enough budgets** to keep up with the acceleration in digital business. In some cases, companies did not build traditional security infrastructure to **expand scope across new and unknown systems**. This lack of planning may cause problems and force security and risk teams to **increase their investment** to keep up with this new demand.

2 Knowledge gap in cybersecurity

On a different topic, but related to a lack of budget, is also the k**nowledge gap in cybersecurity**. As companies continue with new digital initiatives, the cybersecurity team will need to grow, expand their effort, and potentially **get new skill sets** to use Azure cloud and Microsoft 365.

3 Breakable permissions inheritance

If a user creates an ad hoc share to a person outside a group, it can **break the permission inheritance**, creating a vulnerability.
To resolve this issue and reduce the risk, try to **minimize the number of ad hoc shares**. Admins can also set the necessary permissions to be copied to the shared document when the permissions inheritance breaks. You can also limit the number of users sharing content on sites to help reduce the risk.

4 Sharing files without a password

While we're on the topic of sharing documents, another challenge is that a user can share both files and folders with anyone **without requiring a password**. This incident happens when external sharing is set to "on" by default for SharePoint and OneDrive. This default is the permissive setting, allowing employees to share files and folders with anyone outside the organization. This setting means links that don't require sign-in can be transferred, which **implies anyone gets access to the link to use it**.

In most cases, the default setting may be **too permissive**. Instead, you should change the setting to be more in line with your business and security needs. In cases where you **want tighter control**, you can change the external sharing setting. Other options are to share files with new and existing guests, existing guests, or only people in your organization.

5 Microsoft 365 audit log is not real-time

The audit log in Microsoft 365 doesn't capture events in real-time. While events in SharePoint Online and Exchange Online may **appear 30 minutes after the event**, those from Power Apps or Power Automate **don't appear until 24 hours later**.

6 Understaffed and overworked IT can mismanage servers and equipment

With traditional on-premise servers, IT retains **complete control over security**. IT is responsible for setting up user access policies, implementing and maintaining firewalls, antivirus software, and any other type of cybersecurity protection. This responsibility includes ensuring security patches are updated regularly and **protecting against cyber attacks**.

The reality is this control can be both a good and a bad thing. If the business has adequate IT support, then on-premise can help companies know that they can **lock down servers** and **keep their data private**. Unfortunately, on-premise servers can also be mismanaged, making them vulnerable to the latest security threats.

In the cloud, this security is the responsibility of the cloud service provider. You want to choose a cloud service provider like Microsoft Azure that **maintains the latest security controls**. You need to select a provider that supports security at data centers to protect against intruders. This way, you know the software is kept up-to-date and that they are ready for **attacks from cybercriminals** as well as natural disasters. Current cloud providers offer robust security teams and tight procedures to make sure your sensitive data is protected.

Tips and tricks for a good cloud strategy

The reality is that IT organizations have **passed the time** when they need to ask whether they should migrate applications to the cloud. Instead, they need to focus on **accepting the pace** and innovation that cloud providers such as Azure can provide to be the foundation of their business.

Here are some tips and tricks to help you create a good cloud strategy:

Get visibility into your cloud inventory

Cloud inventory visibility is an often overlooked yet critical aspect of **managing your cloud costs**. It allows you to determine the usage of specific resources. It helps **prevent overspending** on those that aren't being used by ensuring they are stored appropriately and have actionable workflows in place if needed or terminated when done.

With visibility into the cloud, you can **get alerts about these unused instances**. You'll know just how much money could be saved based on data gathered during this process, which will help keep unnecessary spending at bay.

Automate M365 governance processes

Take the burden of enforcing governance off your admins with automated governance workflows.

With SysKit Point, you can automate your M365 governance workflows. It lets you run audit reports that track user and admin activity across your tenant and have a **complete understanding of all permissions and memberships**. You can periodically review who has access to what and make owners responsible for maintaining access to their resources.

Use easy-to-follow cost management strategies

To optimize your cloud strategy, you must understand who will be using the service and how. Clear guidelines for cost management policies can **help guide this process** and lay out rights in controlling changes or optimizing infrastructure. It would be **best to automate these rules** so they are followed with minimal hassle when they're necessary.

Utilize autoscaling

Autoscaling is a great way to **increase application uptime** without increasing costs. It allows you to **scale up and down** automatically based on demand metrics. Still, auto-scalers need **clear guidelines** for what those numbers represent.

Use Azure Reserve Virtual Machines

The next time you need to buy a new virtual machine, try out Azure Reserved Virtual Machine Instances. The prepaid reservations will **reduce costs by up to 72%** and help keep your data secure.

Improve security and ensure compliance

It would be best if you tracked the activities of administrators as well as end-users in your tenant. SysKit Point lets you **audit M365 user access**, external sharing, Microsoft Teams, M365 Groups, Exchange Online, and OneDrive. You can troubleshoot errors and **pinpoint the time and place** the issue occurred and the user responsible. In case of suspicious activities, you can have SysKit Point send alerts to help you avoid serious data breaches.

SysKit Point lets you audit M365 user access, external sharing, Microsoft Teams, M365 Groups, Exchange Online, and OneDrive. You can troubleshoot errors and pinpoint the time and place the issue occurred and the user responsible.

What's essential for the success of an M365 cloud strategy?

While companies may **embrace and sanction cloud services**, the challenge may be those hidden shadow IT services about which you don't know. While the number of sanction services may be small, **unsanctioned services can be huge**. This size difference is why determining the scope of your cloud consolidation is an excellent first step.

1 DETERMINE THE SCOPE

This reality is why it's essential to **discover the scope** of your unsanctioned services as you begin the cloud consolidation process. To find the shadow IT web applications currently in use, you can use the Microsoft cloud app security. You can use **automated discovery tools** to help you find current software. Microsoft Cloud Security can also be helpful. You may also need to do some endpoint auditing.

You can use all of these methods to look for standard solutions that may have **overlapping capabilities** with Microsoft 365.

While there may be some manual effort in **discovering the shadow IT services**, you can also use automated discovery to help complement these efforts. Another way to find out what shadow IT services exist is to **interview different business groups** and ask them what cloud services they are currently using to perform their work.

2 CREATE A REFERENCE IT STRUCTURE FOR CLOUD

Once you have the analysis from the first step, you'll better understand what everyone is using and its purpose. You may uncover numerous cloud services that you can eliminate as part of this consolidation. There may also be a way to integrate complementary services if features in the external services are not available in Microsoft 365.

In this process, it's important to remember that you have business units involved, and it's not strictly an IT decision. It's essential to get buy-in from management in different business units.

It may be that business managers need better education to see the possibilities available in Microsoft 365. These possibilities may require additional education for various business units for different business scenarios, preferences, and requirements.

CREATE A BUSINESS CASE

3

When you get to this step, you want to create a business case for cloud consolidation. This step involves understanding the current state as well as the ideal future state. This business case will depend on the level of changes you're planning to advocate for the organization. Other factors are the investment of money and time that you will require to implement said changes. You'll also need to include the amount of adoption support you anticipate for this cloud consolidation.

You'll need to budget for cloud service fees, migration tools, and consulting support for your migration to cloud. You'll need to establish time frames with the changes required within your business case.

As part of this business case, you'll also want to try and uncover any hidden challenges with data or workflows that may make it difficult to migrate to the cloud. The larger organizations, especially those that span multiple locations or countries, may want to consider cloud migration services.

Conclusion

Microsoft cloud is a natural evolution of business technology. M365 cloud strategy is not just about hosting your data on remote servers. It's about the new ways you can leverage that infrastructure to create competitive advantages for yourself and your company. There are many challenges with moving to the cloud, but these tips and tricks can help.

Contact:

SysKit
Krste Pavletića 1, 10000 Zagreb, Croatia
+44 (0) 20 3322-2034 , +1 (631) 406-4900, +1 (855) 855-5071
sales@syskit.com, www.syskit.com