CAPITALIZING ON CLOUD

5 Core Components of a Successful Azure Cloud Foundation

LUNAVI

Following a year defined by remote workforces, virtual collaboration and unprecedented change, it's not surprising that more companies than ever are making their move to Microsoft Azure and other public clouds to improve efficiencies and accelerate digital transformation.

But in the rush to capitalize on cloud, many companies are skipping critical best practices that are the basis of a successful cloud foundation. The result is often unexpected costs and complexities that can limit cloud success today and future workload expansion.

To help your organization avoid these missteps, learn what's needed to build a strong and effective Azure cloud foundation. The following list will give you a high-level look at the 5 core components your organization should prioritize now to optimize outcomes with Azure cloud, whether you're just getting started or already planning your next step forward.

1 Security & Compliance

Cloud security is all about reducing vulnerabilities that put your company's data, assets and environment at risk. After all, no company wants to be the next headline about a security breach because they didn't properly secure their cloud landscape. In the rush to "get apps out to the market," however, many companies may end up treating security more as an afterthought than an essential part of their cloud foundation.

GETTING IT RIGHT

Making security your first priority is the first step toward ensuring a successful cloud foundation. And, with Microsoft Azure, you'll have ready access to a powerful combination of tools that not only provide comprehensive visibility across your landscape, but also next-gen capabilities that help streamline threat detection and response. It also provides tools to implement a compliance scaffold that's in alignment with industry defining CIS and NIST benchmarks. Keep in mind that tools and technology are only part of the solution, however. You also need the right people involved. Start by including your security team upfront. They bring valuable insight and perspective to the table when it comes to ensuring alignment with your company's overall security and compliance goals. That said, many security professionals may not be fully cloud-aware yet. So, you'll also want to partner with experts who can help translate your on-premises strategies to the cloud to ensure that you strike the right balance between minimizing risk and maximizing results at every stage of your cloud journey.

2 Platform Governance

A governance framework lets you define who has access to what, where, when and how within your cloud landscape while also putting cost guardrails in place to ensure cloud consumption doesn't exceed defined thresholds or quotas. It's the kind of detailed planning that many companies tend to put off due to limited resources, time or in-house expertise. But, without establishing these rules to govern your cloud landscape, it can quickly turn into a Wild, Wild West of computing environments, where things are being stood up in ad hoc way without clear standards, consistency or cost control.

GETTING IT RIGHT

Effective governance is a critical part of your Azure cloud foundation that involves applying best practices around specific standards, from naming conventions to tagging resources and defining role-based access to those resources. To be effective, companies need to do this work upfront to make sure everything is properly implemented, starting with the first application you stand up. The right partner can help you put the right standards in place, based on your overall governance framework. They can also help you establish effective guardrails around them to alert your IT staff to potential issues before they occur, so you minimize over-consumption costs and complication. Plus, this framework gives you a clear blueprint to ensure future app deployments and additional workload expansions are all based on the same standards.

3 Network & Interconnectivity

Even though a mature network landscape isn't required when it comes to deploying applications in the cloud, it can help fend off critical connectivity risks while providing a more consistent, low-latency experience for end users. Despite these advantages, cloud networking can be murky territory for on-premises networking experts. As a result, many companies miss out on opportunities to more fully optimize security and application performance by expanding and integrating their network into the cloud.

GETTING IT RIGHT

For most companies, partnership is key to completing this part of your cloud foundation. Designing and integrating an effective cloud network requires partnership. You want a partner who knows the gotchas and lessons learned of cloud networking and can help you apply best practices to lower connectivity risk, isolate and lower application risk, and minimize app latency. Choose a partner who also understands and can help you integrate the different networking technologies within Azure, including Platform-as-a-Service components.

4 Identity and Access Management

Although often lumped into the main security bucket, Identity and Access Management (IAM) is a distinct pillar within the cloud foundation that focuses specifically on validating user access and authentication. When implemented properly, IAM casts a wide net of integrated "security gates," such as multi-factor authentication, to secure access to data and applications across the IT landscape, whether in the cloud or on premises. What many companies miss, however, is the need to integrate these tools with their overall identity and security strategy in order to both secure cloud and on-premises assets and ensure an optimal user experience.

GETTING IT RIGHT

Azure offers a comprehensive set of services, tools, and reference architectures to enable organizations to create highly secure and operationally efficient environments. However, because many on-premises security teams are unfamiliar with the application landscape and underlying infrastructure of the cloud, working with an experienced cloud expert can help you better understand where and how to apply the right gates to protect both your users and your organization.

5 Monitoring & Management

This final pillar of the foundation is really about operationalizing everything you put into place. Your IT teams need visibility into their cloud environments to ensure their workloads run properly. Achieving the quintessential "single pane of glass" to seamlessly monitor and manage your entire environment is no easy task when it comes to the cloud. Companies need to know their options so they can effectively leverage existing resources more strategically and cost-effectively.

GETTING IT RIGHT

With the right partner, companies can typically choose to either fully outsource management of their cloud environment or secure a hybrid approach that shares these responsibilities upfront but also positions the company to more fully engage the partner as their expansion into the cloud grows. Both of these options can help accelerate growth and success in Azure while freeing critical in-house resources to focus on more strategic initiatives rather than day to day management and monitoring of hardware and software.

At Lunavi, we help companies establish and build on these core components of a successful Azure cloud foundation, no matter where they are in their cloud migration or digital transformation journey. As your partner we make sure you're able to extend properly to achieve the right outcomes for your organization today and in the future. We can help assess your existing teams and provide support and training where needed to ramp up the right level of skills and cloud-aware expertise. We also help integrate proven best practices into current processes to streamline expansion and minimize IT demands and disruption.

LEARN MORE To learn more about how to build an Azure cloud foundation and how Lunavi can help you optimize your cloud, contact us today or visit https://go.lunavi.com/azure-adoption-program.