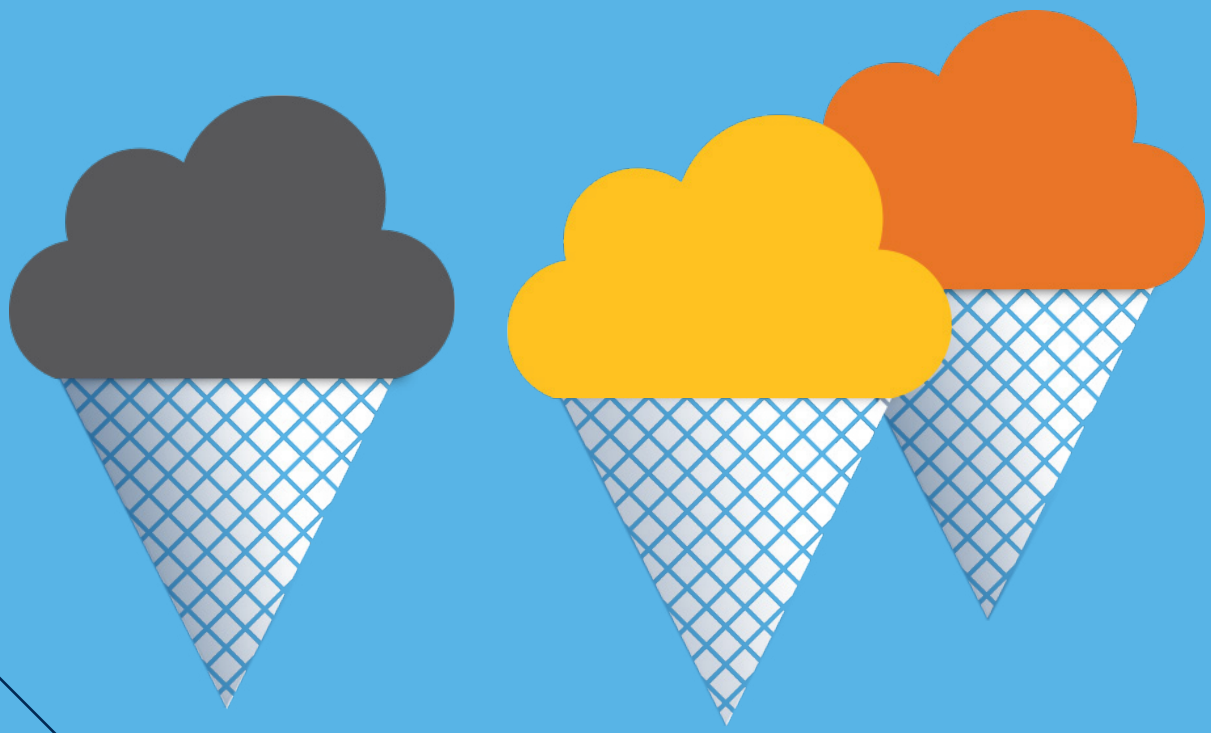
Microsoft Azure

SADA systems

Key Security Considerations:

HOW TO EVALUATE THE DIFFERENT FLAVORS OF THE CLOUD



Key Security Considerations: How to Evaluate the Different Flavors of the Cloud

Gold Microsoft Partner

Just as the cloud provides a different way of managing technology resources and operating your business, the security posture required to protect your data in the cloud is different as well. While cloud service providers (CSPs) generally ensure security OF the cloud, it is the responsibility of customers to properly protect the data that is transacted within it. With different models to choose from -- single cloud platform, multi-cloud, hybrid-cloud -- customers must ask the right questions and perform the necessary due diligence in order to create an appropriate framework for the security of their data and assets.

Identifying the right type of security for your organization presents challenges that require both technology and business thinking. Consider first off that one of the key reasons for migrating to the cloud in the first place is to take advantage of its flexible and dynamic nature; it's an environment that maps to your business needs. Therefore, you can't hermetically seal off your data and functionality to prevent access. The nature of the cloud is that it's an effective enabler of data transactions and communication, both into and out of your enterprise environment. Your business depends upon integration with both internal and third-party applications and the ability to share unique (and usually very sensitive) data with different types of stakeholders. This requires that your data be controlled effectively, but also not totally locked down.

Especially when using multi-cloud and hybrid approaches, you are relying on the easy movement of data to provide business advantages while benefiting from efficient use of IT resources. And remember also that security is not a one-and-done proposition. You certainly apply your security controls in your cloud, but you have to also continuously be aware of the risks and vulnerabilities and ensure you have processes in place to alert and remediate so you can fix issues before they result in your company being the next corporate poster child for data breaches.

Key Security Considerations: How to Evaluate the Different Flavors of the Cloud

As you begin developing your framework for cloud security, consider things like internal policies and requirements, compliance, DevOps, security training, automation, remediation, and other critical elements that are necessary to having a comprehensive security solution for your cloud. We encourage you to learn more about cloud security and how it fits with your organization. The following questions should help you and your team make smarter decisions around how you're going to procure, develop, apply, and manage security for your single, multi, or hybrid cloud environment:

1 Support for Alerts and Remediation

Do your security policies demand that you alert partners and other stakeholders, as well as trigger remediation processes upon detection of security issues? If so, a multi-cloud approach will necessitate integration of security alerts so that the user is aware of issues based on the risk, along with information that identifies which platform and where within the platform the issues lives. Users will want to know first that an issue exists, irrespective of platform. Yet, they also need to know where within your environment the issue is so they can pinpoint it and how it's affecting other parts of the overall environment. Only with a clear view over your entire cloud surface can a user adequately rectify issues.

2 Customizing Security Settings

Do you have the appropriate security settings in place to meet the needs of your company? CSPs offer out-of-the-box security settings that might not be appropriate for your needs. You will need flexibility and management capabilities to property secure your environment and assign controls based upon the risk you're comfortable at each layer of the cloud stack. In hybrid environments, this might mean porting your legacy settings to your new cloud platform, but you will want platforms that make this easy.

3 Security Management

Is security handled by a single team within your organization, or is responsibility handled across your enterprise? For multi-cloud and hybrid environments, it will likely be the latter. It's not uncommon for multi-cloud environments to be formed as a result of different group needs, even within the same organization. Similarly, hybrid solutions maintain legacy assets. Management has to be flexible enough that your security solution can extend to different teams based on their needs, skill levels, and requirements.

Key Security Considerations: How to Evaluate the Different Flavors of the Cloud

4 Security Training

The cloud offers a simpler way of managing technology resources, which offers a major benefit because it maximizes the contributions of more team members. With that in mind, it's critical that there is a training roadmap for whatever security solution you choose to use. How will you handle security skills and training? Not every user will be comfortable with the offerings available. Seek a solution that is user-friendly, innovates seamlessly (e.g., new functionality is deployed without disruption), and comes with training and support.

5 Compliance as a Component of Security

Is compliance a part of your security needs? If so, then it is important to define a strategy that monitors for compliance in different environments. Each platform performs its monitoring a bit differently, and of course, legacy applications and assets usually require independent solutions to perform stress tests and ensure they are in compliance with various standards. It will be critical, no matter how your environment is constructed, to have all cloud assets and applications communicating with one another so no compliance controls are missed.

The goal of security, no matter what platform or environment you use, is to protect your critical data from attacks and from internal misconfigurations. By customizing your organization's security framework to fit your architectural and platform needs, you can be better assured that you will be able to maintain continuous awareness and apply risk mitigation best practices. ▲

SADA Systems, Inc. is a privately-held global leader in providing business and technology consulting services that transform organizations through cloud-based solutions. Named 2017 Microsoft Health Innovation award winner, 2016 Microsoft Partner of the Year Finalist for Cloud Productivity, 2015 Microsoft Partner of the Year for Cloud Packaged Solutions and three-time U.S. Education Cloud Partner of the Year, SADA Systems is a Microsoft Cloud Solutions Provider (CSP), holding multiple Gold competencies.

SADA systems

NOW THAT YOU'VE READ THE 5 KEY CONSIDERATIONS THAT YOU AND YOUR COMPANY NEED TO DISCUSS BEFORE DEVELOPING YOUR SECURITY STRATEGY, IT'S TIME FOR A CHAT.

SADA Systems has a proven track record in enterprise consulting, cloud platform migration, custom application development, managed services, user adoption and change management.

With a certified team of Microsoft Partner Professionals (P-Sellers), SADA successfully delivers on all Microsoft cloud solutions, including Microsoft 365, Office 365, SharePoint Online, Teams, Skype for Business, Power BI, Dynamics 365, Enterprise Mobility + Security, and Azure.

Do you have questions about how to best optimize your cloud security strategy? Our Cloud solution experts are here to help. Take advantage of a FREE strategy session today.

BOOK STRATEGY SESSION

http://info.sadasystems.com/microsoft-azure-evaluating-the-cloud-ty

@SADASYSTEMS
/SADASYSTEMSINC
SADA-SYSTEMS
+SADASYSTEMS
WWW.SADASYSTEMS.COM
MSSALES@SADASYSTEMS.COM

Microsoft Azure