**Syllabus**

**UNIT 6 :Cloud Security & Implementation of Cloud**

* 1. Cloud Security Fundamentals
  2. Cloud Security Architecture
  3. Cloud Computing Security Challenges
  4. Privacy and Security in Cloud
  5. Identity Management and Access control
  6. Demonstrate the commercial cloud computing Infrastructures
  7. Introduction to Dockers Container

Case Study’s based on Cloud Computing Concepts.

**Cloud Security Fundamentals: 3 Steps to Build Your Strategy**

Follow these steps to learn the basics of securing data on popular clouds including Google, Azure, and AWS.

There are many reasons why enterprises are using cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to facilitate web applications. Outsourcing to the cloud adds scalability, efficiency, and reliability, while also reducing workloads for IT teams.

These are positives, for sure – but while enterprise IT leaders celebrate the benefits that the cloud brings to their businesses, they may be missing a big negative. Organizations that move critical infrastructure to cloud platforms often mistakenly assume that their cloud providers also lock down security. In fact, this is often not the case; and when enterprises let critical cloud security slip, their security teams may also fail to configure critical controls or adopt the necessary secure architecture practices, leaving gaps that attackers can compromise.

For example, many of the risks that security teams have to deal with when they're working to keep attackers from breaching on-premises architecture – like improper segmentation, overly permissive firewall rules, or weak passwords – also exist in the cloud. And there are always new risks that can affect cloud platform security, such as exposure of API keys in source repositories or open web directories. None of these risks should be left unmonitored – yet the default configurations for AWS, Azure, and GCP often don't include turning on event logging, encryption, data retention, multifactor authentication, and other preventative controls.

The steps below detail how to configure and monitor your cloud platforms for improved visibility, which cloud-native tools are needed to secure cloud platforms, and why integration can help secure a multi-cloud environment.

**Step 1: Determine where sensitive data lives, and prioritize integrations that increase visibility**

Because cloud deployments are relatively easy, it’s also easy to move data around from cloud to cloud. For this reason, security teams need to understand where data is stored and how it's used. Without this knowledge, and without controls that manage visibility into sensitive data, it could be painfully easy to transfer customer data from a private server to a public storage repository.

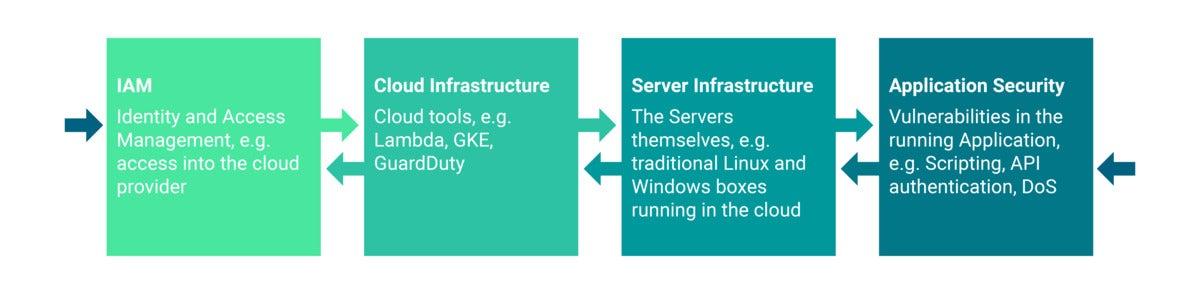
Typically, the flow of data in the cloud should be traced from the point where the application is accessed, and back to where a company’s developers eventually access the systems on which data is stored. Security teams need knowledge of how data moves through the environment – if not, they'll waste time and money securing potentially lower-priority infrastructure devices.

Fortunately, the major cloud platforms have out-of-the-box security tools and open APIs that make log ingestion easy. Once security teams know what they're looking for, they can use proper tuning and integrations to make alerting and visibility into attacks as simple as managing on-premises tools.

**Step 2: Configure cloud platforms to maximize the security of their architecture**

It's worth spending time to figure out which features a specific cloud platform already provides for visibility and automation. Once these basic tools are enabled, security experts can start the process of fine-tuning and tightening controls. For example, teams can set up alerts for unusual calls from accounts, repeated denies, policy changes, and other actions and content that help pinpoint attacker activity.

At this stage, review the areas of vulnerability that can allow bad actors to pivot their attacks, including Identity Access Management (IAM), cloud infrastructure, server infrastructure, and application security. Application security and IAM should be the primary areas of concern. IAM can be secured through the combination of access logs and regular auditing and tightening of permissions; application security requires security by design, via developers who care about the security of their applications.

[](https://images.idgesg.net/images/article/2021/02/cloud-security-blog-image-100875709-orig.jpg?auto=webp&quality=85,70)

**Step 3: Monitor the cloud through integration**

Most cloud environments generate a large number of logs that can quickly take up all of a security team's time. To constantly parse, tune, and respond to alerts, teams need automation and integration.  To efficiently and effectively respond to alerts, teams need a centralized view of their data across cloud and on-premises environments, such as through an [Open XDR solution](https://www.reliaquest.com/blog/how-we-got-here-will-open-xdr-finally-unify-our-security-environment/). And, to see what’s happening in the cloud environment and export logs into an alerting engine such as a SIEM, enterprise organizations need to plan a cloud-logging strategy by answering these questions:

* **Where will log aggregation and filtering tools reside?**It’s efficient to have collection tools doing the filtering and aggregating as close to the source as possible.
* **How big are the Internet connections between your cloud environment and local data centres?**It may be more cost-effective to keep raw data at both places, and send actionable events used in alerting rules to the central SIEM or monitoring tool.
* **How will you collect and parse cloud infrastructure logs?**In addition to standard operating system or application logs from servers, many essential cloud infrastructure logs should be gathered and monitored for unauthorized or malicious activities.

Cloud Computing Security Architecture

**Security in cloud computing is a major concern. Proxy and brokerage services should be employed to restrict a client from accessing the shared data directly. Data in the cloud should be stored in encrypted form.**

Security Planning

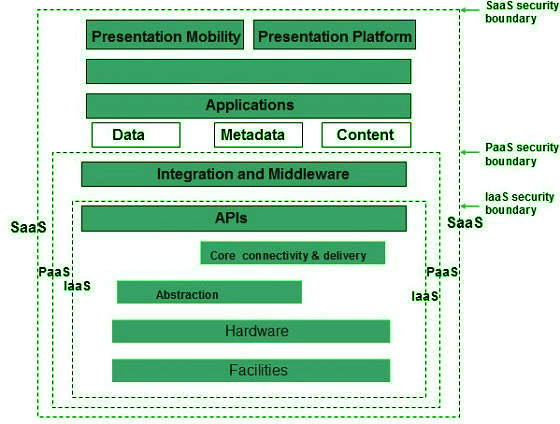
Before deploying a particular resource to the cloud, one should need to analyze several aspects of the resource, such as:

* A select resource needs to move to the cloud and analyze its sensitivity to risk.
* Consider cloud service models such as **IaaS, PaaS,**and These models require the customer to be responsible for Security at different service levels.
* Consider the cloud type, such as **public, private, community**, or
* Understand the cloud service provider's system regarding data storage and its transfer into and out of the cloud.
* The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Security of Cloud

Security Boundaries

The **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate. A particular service model defines the boundary between the service provider's responsibilities and the customer. The following diagram shows the **CSA stack model:**



Key Points to CSA Model

* IaaS is the most basic level of service, with PaaS and SaaS next two above levels of services.
* Moving upwards, each service inherits the capabilities and security concerns of the model beneath.
* IaaS provides the infrastructure, PaaS provides the platform development environment, and SaaS provides the operating environment.
* IaaS has the lowest integrated functionality and security level, while SaaS has the highest.
* This model describes the security boundaries at which cloud service providers' responsibilities end and customers' responsibilities begin.
* Any protection mechanism below the security limit must be built into the system and maintained by the customer.

Although each service model has a security mechanism, security requirements also depend on where these services are located, private, public, hybrid, or community cloud.

Understanding data security

Since all data is transferred using the Internet, data security in the cloud is a major concern. Here are the key mechanisms to protect the data.

* access control
* audit trail
* certification
* authority

The service model should include security mechanisms working in all of the above areas.

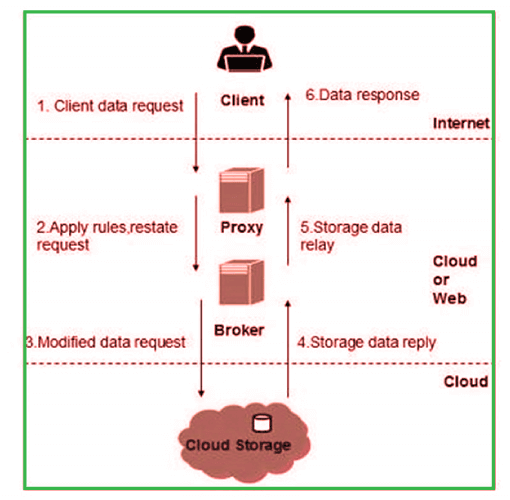
Separate access to data

Since the data stored in the cloud can be accessed from anywhere, we need to have a mechanism to isolate the data and protect it from the client's direct access.

**Broker cloud storage** is a way of separating storage in the Access Cloud. In this approach, two services are created:

1. A broker has full access to the storage but does not have access to the client.
2. A proxy does not have access to storage but has access to both the client and the broker.
3. Working on a Brocade cloud storage access system
4. When the client issues a request to access data:
5. The client data request goes to the external service interface of the proxy.
6. The proxy forwards the request to the broker.
7. The broker requests the data from the cloud storage system.
8. The cloud storage system returns the data to the broker.
9. The broker returns the data to the proxy.
10. Finally, the proxy sends the data to the client.

**All the above steps are shown in the following diagram:**



Encoding

Encryption helps to protect the data from being hacked. It protects the data being transferred and the data stored in the cloud. Although encryption helps protect data from unauthorized access, it does not prevent data loss.

Why is cloud security architecture important?

The difference between "cloud security" and "cloud security architecture" is that the former is built from problem-specific measures while the latter is built from threats. A cloud security architecture can reduce or eliminate the holes in Security that point-of-solution approaches are almost certainly about to leave.

It does this by building down - defining threats starting with the users, moving to the cloud environment and service provider, and then to the applications. Cloud security architectures can also reduce redundancy in security measures, which will contribute to threat mitigation and increase both capital and operating costs.

The cloud security architecture also organizes security measures, making them more consistent and easier to implement, particularly during cloud deployments and redeployments. Security is often destroyed because it is illogical or complex, and these flaws can be identified with the proper cloud security architecture.

Elements of cloud security architecture

The best way to approach cloud security architecture is to start with a description of the goals. The architecture has to address three things: an attack surface represented by external access interfaces, a protected asset set that represents the information being protected, and vectors designed to perform indirect attacks anywhere, including in the cloud and attacks the system.

The goal of the cloud security architecture is accomplished through a series of functional elements. These elements are often considered separately rather than part of a coordinated architectural plan. It includes access security or access control, network security, application security, contractual Security, and monitoring, sometimes called service security. Finally, there is data protection, which are measures implemented at the protected-asset level.

A complete cloud security architecture addresses the goals by unifying the functional elements.

Cloud security architecture and shared responsibility model

The security and security architectures for the cloud are not single-player processes. Most enterprises will keep a large portion of their IT workflow within their data centers, local networks, and VPNs. The cloud adds additional players, so the cloud security architecture should be part of a broader shared responsibility model.

A shared responsibility model is an architecture diagram and a contract form. It exists formally between a cloud user and each cloud provider and network service provider if they are contracted separately.

Each will divide the components of a cloud application into layers, with the top layer being the responsibility of the customer and the lower layer being the responsibility of the cloud provider. Each separate function or component of the application is mapped to the appropriate layer depending on who provides it. The contract form then describes how each party responds.

**5 Key Cloud Computing Security Challenges**

Today’s businesses want it all: secure data and applications accessible anywhere from any device. It’s possible with cloud technology, but there are inherent cloud computing security challenges to making it a reality.

What can enterprise businesses do to reap the [benefits of cloud technology](https://www.cdnetworks.com/cloud-security-blog/what-is-cloud-security-and-what-are-the-benefits/) while ensuring a secure environment for sensitive information? Recognizing those challenges is the first step to finding solutions that work. The next step is choosing the right tools and vendors to mitigate those **cloud security challenges**.

In our technology driven world, security in the cloud is an issue that should be discussed from the board level all the way down to new employees. The CDNetworks blog recently discussed “[what is cloud security](https://www.cdnetworks.com/cloud-security-blog/what-is-cloud-security-and-what-are-the-benefits/)” and explained some of its benefits. Now that we understand what cloud security is, let’s take a look at some of the key challenges that may be faced and why you want to prevent unauthorized access at all costs.

**Challenge 1: DDoS and Denial-of-Service Attacks**

As more and more businesses and operations move to the cloud, cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks are more common than ever before. Verisign reported IT services, cloud platforms (PaaS) and SaaS was the most frequently targeted industry during the first quarter of 2015.

A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a [DDoS attack](https://www.cdnetworks.com/cloud-security-blog/tips-to-protect-your-business-from-ddos-attacks/) is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.

Complementing cloud services with [DDoS protection](https://www.cdnetworks.com/cloud-security/flood-shield/) is no longer just good idea for the enterprise; it’s a necessity. Websites and web-based applications are core components of 21st century business and require state-of-the-art cybersecurity.

**Challenge 2: Data breaches**

Known data breaches in the U.S. hit a record-high of 738 in 2014, according to the Identity Theft Research Center, and hacking was (by far) the number one cause. That’s an incredible statistic and only emphasizes the growing challenge to secure sensitive data.

Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in all scenarios including private cloud, public cloud, and hybrid cloud situations), some of those security controls are relinquished to a trusted partner meaning cloud infrastructure can increase security risks. Choosing the right vendor, with a strong record of implementing strong security measures, is vital to overcoming this challenge.

**Challenge 3: Data loss**

When business critical information is moved into the cloud, it’s understandable to be concerned with its security. Losing cloud data, either through accidental deletion and human error, malicious tampering including the installation of malware (i.e. DDoS), or an act of nature that brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.

To face this challenge, it’s imperative to ensure there is a disaster recovery process in place, as well as an integrated system to mitigate malicious cyberattacks. In addition, protecting every network layer, including the application layer (layer 7), should be built-in to a cloud security solution.

**Challenge 4: Insecure access control points**

One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and particularly the application programming interfaces (APIs) users interact with aren’t secure? Hackers can find and gain access to these types of vulnerabilities and exploit authentication via APIs if given enough time.

A behavioural [web application firewall](https://www.cdnetworks.com/cloud-security/application-shield/) examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications and APIS from security breaches within cloud environments and data centers that are not on-premises.

**Challenge 5: Notifications and alerts**

Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud computing security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough data security and access management plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

**Final Thoughts on Cloud Security Challenges**

Cloud computing security issues and challenges are not insurmountable. With the right cloud service provider (CSP), technology, and forethought, enterprises can leverage the benefits of cloud technology.

CDNetworks’ cloud security solution integrates web performance with the latest in cloud security technology. With 160 points of presence, websites and cloud applications are accelerated on a global scale and, with our cloud security, our clients’ cloud-based assets are protected with 24/7 end to end security, including [DDoS mitigation](https://www.cdnetworks.com/cloud-security-blog/ddos-mitigation/) at the network and application levels.

**Data Privacy & Security in Cloud Computing**

 Cloud technology has given opportunities to many businesses to showcase their potential in the business world. SMEs are not only getting an opportunity to grow, they are also taking their business operations to the next level. ***Cloud technology*** has opened a door for small & medium scale companies to acquire market share by entering the yard of bigger players. As the business requirements have become on-demand and need-based, it gave many companies a significant edge and allow them to complete in a much larger business space.

***Cloud technology*** provides various advantages. Starting from data management, data storage, 0% downtime, CRM management, resource optimization to entire business automation. It also reduces a high amount of investment and saves a lot of time.

At the same time, cloud computing has raised multiple eyebrows with IT management, especially when it comes to ***data security in the cloud computing***. ***Data security*** and privacy protection are two major factors. These two factors are becoming more important for the future development of cloud computing technology in business, industry, and government. While addressing this fear, Google claimed that data stored in the cloud are much safer.

*If someone asks me what cloud computing is, I try not to get bogged down with definitions. I tell them that, simply put, cloud computing is a better way to run your business.*

-Mark Benioff, CEO of Salesforce

**What are the Challenges?**

Data Replication

Every business faces this challenge. Snapshots and data backups are taken on a daily basis. They automatically stored in the cloud. Are you aware where they have been stored and who can see and access them? Can you identify and control unauthorised copying of your data?

Data Loss

Data loss can be a disaster for any business. Virtual data can be easily lost or exposed as it moves between VMs or in the cloud. Are you sure that authorised users are accessing your data within predefined policies? Do you have the authority to block any user who is violating data use policies?

New Class of Users

Cloud computing need cooperation between security, storage, application, and security admins. They all manage your sensitive business data. With more number of users, the risk also increases. If one admin went wrong, entire data in the system will be at risk.

Insecure APIs

Application Programming Interfaces (API) allow users to customize their cloud computing practices. APIs can be a threat to ***cloud security*** because of their nature. APIs give developers the tools to build solutions to integrate their applications with other software. The vulnerability of an API depends on the communication that takes place between applications. While this can help developers and businesses, they also issue serious security concerns.

Internal Threat

Never keep this point out of your mind. You may be thinking data is safe inside. But this is one of the biggest challenge company’s face. Employees can use their access to an organisation’s cloud-based services to misuse or access information related to finance, customer details etc.

**How to Protect your Data?**

You can protect your business data in the cloud from unauthorised access. All you need is a sharp eye and an extra effort. Here are few practical tips to keep your cloud data safe and secure.

Always keep backup locally

When it comes to business data, you have to be extra conscious. Always have a backup for your data. It is always good to create hard copies of your business data and keep it with yourself so that you can have access them even if you lost the original one. You can use any cloud storage solutions to store your data. You can set up a cloud account & can keep the backup copies. You have another option of keeping the backup data in an external storage device also like a hard disk or a thumb drive. This will allow you to access the information even if without the internet.

Don’t store sensitive data

Technology is changing. Businesses are also changing as per the technology. Data is playing an important role in businesses today. So, data privacy is one of the primary aspects of any business. But if something is there on the internet, it is hard to trust it is safe. So, one should avoid storing the most sensitive files or information in the cloud. Identity theft is on rising and you can’t take any risk. You should keep those files in cloud platform which you access frequently and should avoid putting information related to financial details, competitor details, client details, contact details like phone number/address etc. If you are keeping these files, make sure you encrypt them before uploading.

Data encryption

One of the best ways to protect your data while using cloud storage is to do data encryption. This is the best form of security because you need decryption before accessing the data. This will protect data against service providers and users also. To make it more protected, you can also ensure cloud encryption during uploading and downloading phases. But, this will make data sharing and sync in the cloud platform little slow.

Encrypted cloud service

There are few ***cloud services*** which provide local encryption and decryption of your files and information inside that other than storage and backup. This means the service takes care of both encrypting your files and storing them safely in the cloud. This will ensure that no one including the service provider or the administrators can have the access to your data files. There are many free versions and also trial versions available in the market. You can use them to learn how it works and later can upgrade to enjoy more space.

Using password

The first thing which can be done is to put strong password which can stand a hacking. You can take the help of internet to learn how to create a strong password. It is very important to change your password frequently and never use the same password for all the accounts or folders. You can opt for 2-step verification for login if your cloud service offers that option. Google drive use 2 phase log in option, consist of password & code sent to the registered number. This added security will make your data much safer.

Keep an eye on what you do online

The security of your cloud data largely depends on your online behaviour. While using a public computer, never save your password, and always ensure that you logged out properly. Another biggest concern is accessing cloud data in unsecured or open Wi-Fi hotspots. Such connections are unencrypted, hackers can target your data easily. Never save your password in any of the public forum or social media. Change Wi-Fi passwords frequently.

Anti-virus is a must

Sometimes the weakest link happens to be the computer or device you use for cloud data access. You need to put proper protection in your system/device. It will help in securing your business data. If you expose yourself to bugs and viruses, hackers can access your system easily. You need to choose a very effective and robust anti-virus system for your system, which will protect all the files and information inside that. If your system isn’t well protected, and if the system is not encrypted and secured from bugs, hackers can get hold of your information.

Read your user agreement

If you are new to the world of cloud computing and not sure what cloud storage to choose or how it really work, you have to read the user agreement of the service you are going to sign up for. Initially, it will be difficult to understand and at times it will test your patience, but you need to face this. User agreements always carry essential information which can help you understand things in detail.

Access limitation

Give access to those users who really need. Internal users and third party vendors should only get access to those files which will help them to do their jobs. Use encryption keys if required. Make sure to evaluate the users and vendors regularly and add/remove users as per the requirement.

Platform, control & service monitoring

Platform, control & services monitoring is usually performed as a dashboard interface and makes it possible to identify the operational status of the platform being monitored at any time. Each operational element which is monitored provides an operational status indicator. This helps in determining which elements are performing as per the established standards. By identifying such problems, you can take defensive actions to prevent loss of data or service.

***Cloud data security*** is enhanced with regular patching and upgrading of systems and application software in the cloud platform. New patches, updates, and service packs for the operating system are required to maintain high-end security levels and support new versions of installed products. You have to be committed enough to identify the market trends and new software versions and communicate gaps in security that can appear in installed systems and applications.

***Cloud services*** can give you the best solutions for your business related problems when you are assured that your & your customers data are private and secure. This should be the primary focus for cloud service providers. There are many legal & regulatory challenges which needs to be addressed when data moves from one country to another.

Multinational Framework on privacy and security :

Uncertainty about the legal and regulatory obligations related to data will increase with the increase of the data in the cloud platform. To ensure every business and country get full advantage of cloud computing, different countries have to cooperate to develop a multinational framework on data privacy and security in the cloud. As cloud computing evolves, and data flows from one country to another. For example, data has been created in India using a software hosted in UK & stored in US with users based in Australia. Cloud provider needs to coordinate this entire process to make sure the data flow is going smooth & safe.

Rules on Cross-border data transfers :

To enhance the efficiency and security of ***cloud solutions*** and deliver quick results, cloud service providers must be able to operate datacentres in multiple locations and transfer data freely between them. Smooth data flow allows cloud providers to optimize their service and deliver the best business solutions. However, restrictions on cross-border data transfers can create uncertainty if the rules or the legal framework are not followed.

Conflicting legal obligations :

Different governments have different policies when it comes to data flow in their country. Cloud providers will be in legal trouble if they won’t follow the predefined cyber laws. Divergent rules on privacy, data retention, law enforcement access and other issues can lead to ambiguity. For example, one country might have certain rules when it comes to cloud data storage, which might be in direct conflict with another country or a particular service provider.

In order to protect data in the cloud platform, you need to keep all these above things in mind.

**Conclusion**

Cloud computing is one of the most promising technology for the next generation of IT applications. The primary concern toward the accelerated growth of cloud services is data security and privacy issues. The main goal for any company is to reduce data storage and cost associated with it. As we all know data is playing a bigger role in taking business decisions, no company will deploy all their business data into the cloud unless they trust it completely. There are many techniques which have been introduced by IT researchers for data protection and to achieve the highest level of data security. However, there are still certain gaps to be filled by making these methods more effective. More awareness is required in the area of cloud computing to make it acceptable.

Cloud computing purely targets on cost-effective solutions and is a significant promoter of the modern digital economy by enabling leading companies to innovate, operate and conduct business more promptly and efficiently. However, the cloud is more than just delivering cost-effective solutions.

If you expect your business to grow, you are short on capital, or you don’t have technology expertise, **cloud computing** could be the solution. It can add real value and can take your small business to the enterprise level.