Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

·**Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

·**Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

· Information security protects the integrity and privacy of data, both in storage and in transit.

· **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

·**Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

·**End-user education addresses** the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Cyber Security Features

1. Good analytics

Every organization in every industry can benefit from good analytics. It's easier to put your finger on a threat if you've rated your risks, and have a good historical picture of where your risks have been in the past. When you have good data, you can clearly see your risk, monitor situations that could pose a threat, and move quickly when there's an issue. In fact, good data can help you even after a data breach or attack. Ponemon's 2019 Cost of A Data Breach report found that companies that use security analytics reduce the cost of data breaches by an average of $200,000.

2. Coverage of your biggest external threats

Many threats come from outside your organization. Ponemon's 2018 State of Cyber security in Small & Medium Size Businesses (SMBs) report found that 37% of incidents were confirmed attacks from an external source. These external threats tend to take the

form of hacking and phishing, and tend to come into an organization in a variety of ways: stolen credentials, Denial of Service, compromised web applications, and email attachments. (For example,93% of spam emails are now vehicles for ransom ware). Your security platform should be able to monitor your threats, and let you know when your organization has been compromised or targeted by malicious activity.

3. A defense against internal threats.

While most of an organization's threats tend to come from outside, occasionally the call is coming from inside the house. According to **Egress's Insider Data Breach survey**, 95% of businesses are worried about an insider breach. This doesn't necessarily mean you've got bad actors in your organization — most of the time internal threats are mistakes (like misconfiguration of AWS buckets or unapproved workarounds) or bad choices by employees. Occasionally, however, an internal actor will get involved with truly malicious activity like espionage or theft — Egress found that 61% of IT leaders believe their employees put sensitive company data at risk maliciously in the last year. Whatever their reasons for exposing you to risk, a good cyber security platform should be able to quickly alert you to mistakes or misuse that could be putting your data or networks at risk.

4. Compliance

Information security means different things in different industries. Every industry and organization — from healthcare to finance – has a unique set of regulations, standards, and best practices when it comes to information security. Your cyber security platform should help your organization achieve, maintain and prove compliance with whatever regulations are relevant to your industry and geographical location.

5. Manage risk across your entire ecosystem.

Third parties — your vendors, partners and contractors — are critical sources of risk to your business. They often have access to your data and networks, but you can't always require them to adhere to specific standards or best practices. It's no surprise that third parties are a significant source of risk — Ponemon's 2019 Cost of A Data Breach report

found that when third parties cause a breach, the cost increases by more than $370,000. Yet, according to Protoviti's 2019 Vendor Risk Management BenchMark Study, only 4 in 10 organizations have a fully mature vendor risk management process in place. Your cyber security platform should let you monitor and manage the risks posed by your vendors. Your cyber security platform must allow you to monitor and manage risk no matter where it occurs — outside the company, inside your organization, or in your supply chain.

6. Threat prevention, detection, and response.

Last year, a survey published in CISO magazine found that 31% of CISOs want their security platform to block more than 95% of attacks and track those attacks they can't block, providing continuous alerts so that the security team can track down the suspicious activity and eliminated it.

7. Continuous monitoring.

When it comes to cyber security, it's no good relying on snapshots of your risk, or compliance. Yes, you and your vendors might be compliant right now, but tomorrow, a patch might not be installed in a timely manner, or someone might misconfigure a server. A security platform that doesn't provide continuous monitoring is leaving holes in your compliance and leaving you opens to risk.

How Security Scorecard can help

Your cyber security platform should be able to keep you apprised of your risk is at all times. Security Scorecard's cyber security platform allows you and your organization's business stakeholders to enable users to continuously monitor the most important cyber security KPIs for your company and your third parties. Our security ratings use an easy-to-understand A-F scale across 10 groups of risk facts with 92+ signals so you can see, at a glance, where your problems are and what actions you should take when any issues are discovered.

By monitoring the cyberhealth of your extended enterprise, you'll be able to collect data on your cyber security efforts and make informed security decisions in the future.

PAAS Services by Clouds

AWS as a Platform as a Service

This service that provides the foundation for developers to design apps. In its simplest sense, a third-party vendor will provide hardware and software tools to users over the Internet, and users will only need to handle the application design and development process. All hardware and software will be hosted by the PaaS service provider on its own infrastructure.

Among 3 Amazon service solutions that apply cloud computing technology namely Iaas Paas Saas AWS, PaaS plays an important role in simplifying the application development process on the web. With cloud technology, developers can access the platform data from anywhere. This can facilitate project development on a global scale. However, it also means that the developers will have less control over the application design environment.

A platform as a Service (PaaS) removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other heavy lifting involved in running your application. PaaS provides the infrastructure and application development platform to easily develop applications over a cloud platform. AWS Lambda is the most robust service that positions as a strong PaaS, enabling developers to utilize all AWS platform services.

AWS offers several services that customers can easily integrate to create a PaaS. For example:

- **AWS Cloud9**: This cloud-based integrated development environment is used to develop applications.

- **AWS CodePipeline**: Developers can use this tool to build and deploy applications. It supports deployment to a variety of AWS hosting options, such as EC2 virtual machines, or containers on Amazon Elastic Container Service.
- **AWS CodeDeploy**: This deployment service enables enterprises to automate deployments to various AWS compute services.
- **AWS Elastic Beanstalk**: Developers use this tool to upload code for web apps and service. AWS handles the deployment, provisioning and load balancing.

Compared to the other major cloud vendors, AWS offers the least integration between its various PaaS-related services. To provide PaaS features, users must connect several services together to build a complete application development and deployment pipeline. This approach appeals to organizations that prefer to pick and choose their tooling, but they must familiarize themselves with multiple AWS offerings and take steps to integrate them.

PaaS Benefits:

- Availability of application development environment which saves users a lot of time and money
- Users don't need to worry about platform maintenance and backup services which are entirely managed by cloud technology
- The infrastructure is stored directly in the cloud, and users can always access it immediately
- Save time developing applications thanks to existing cross-platform environments
- Flexible development according to users' need of using advanced software

PaaS Characteristics

Consider the below characteristics will help you determine when PaaS is being utilized:

- Resources can easily be scaled up or down as your business changes
- Provides a variety of services to facilitate the development, testing, and deployment of apps
- Multiple users can access via the same development application
- Able to integrate with web services and databases

When to Use PaaS

If you are looking for a cost-effective and time-saving solution, PaaS can be an ideal choice. PaaS saves the developer more time to focus on the creative side of app development such as creating, testing, and deploying the app while not having to worry about managing software updates or security patches.

AWS PaaS Drawbacks

- dependent on the provider's functional capabilities, speed, and reliability
- compatibility problems may arise when existing infrastructure is incorporated into a new environment
- security risks due to its availability in the public environment

PaaS examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.

Microsoft Azure as a Service (PAAS)

Platform as a service (PaaS) is a deployment and development environment within the cloud that delivers simple cloud-based apps to complex, cloud-enabled applications. PaaS is designed to support the complete web application lifecycle of building, testing, deploying, managing, and updating.

PaaS includes a complete infrastructure of servers, storages, networking, and middleware development tools like business intelligence services (BI), database management systems, etc. A complete platform is offered in PaaS in which the client can host their applications without the need to worry about the maintenance of the servers and its operating systems. However, the user of the PaaS service should look after the implementation of the developed application to decide whether to scale it up or down depending on the traffic that the application receives.

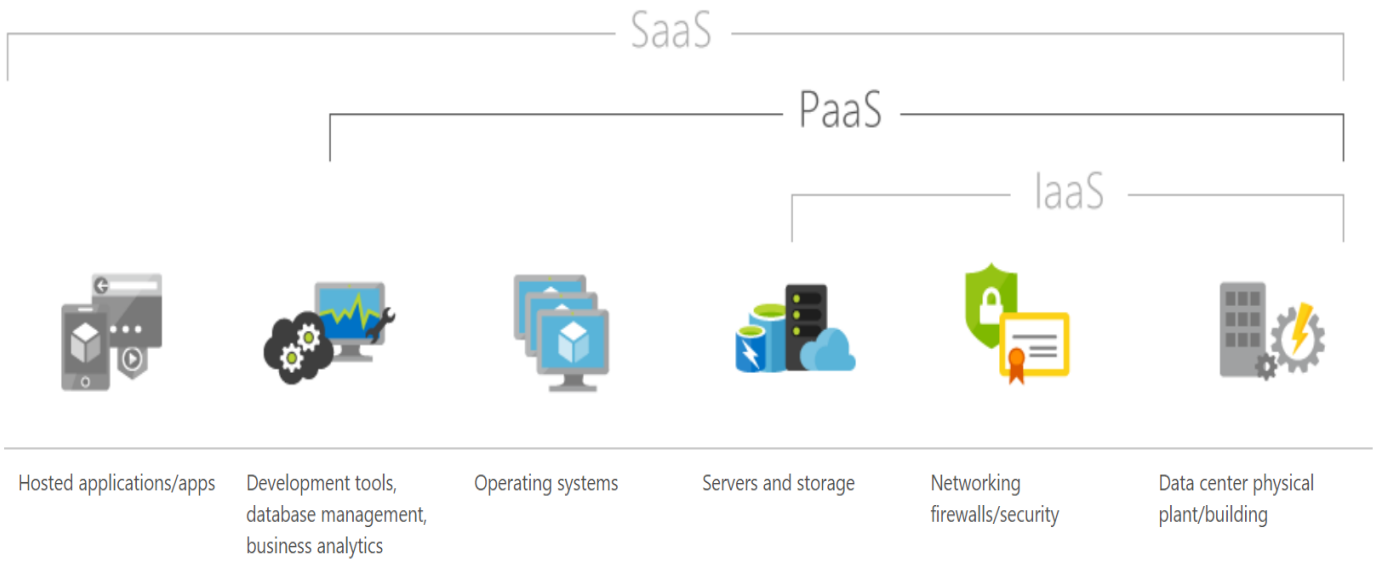


Fig. Microsoft

The PaaS backbone utilizes virtualization techniques, where the virtual machine is independent of the actual hardware that hosts it.

Azure Cloud Services has two main components; the application files such as the source code, DLL, etc. and the configuration file. Together these two will spin up a combination of Worker Roles and Web Roles. On the cloud services, Azure handles all the hard work of the operating systems on your behalf, so that the full focus is to build a quality application for the end users.

The Web Role is an Azure VM that is preconfigured as a web server running IIS (Internet Information Service) which automatically loads the developed application when the Virtual machine boots up. This results in the creation of the public endpoint for the application which is usually in the form of a website but could be an API or similar.

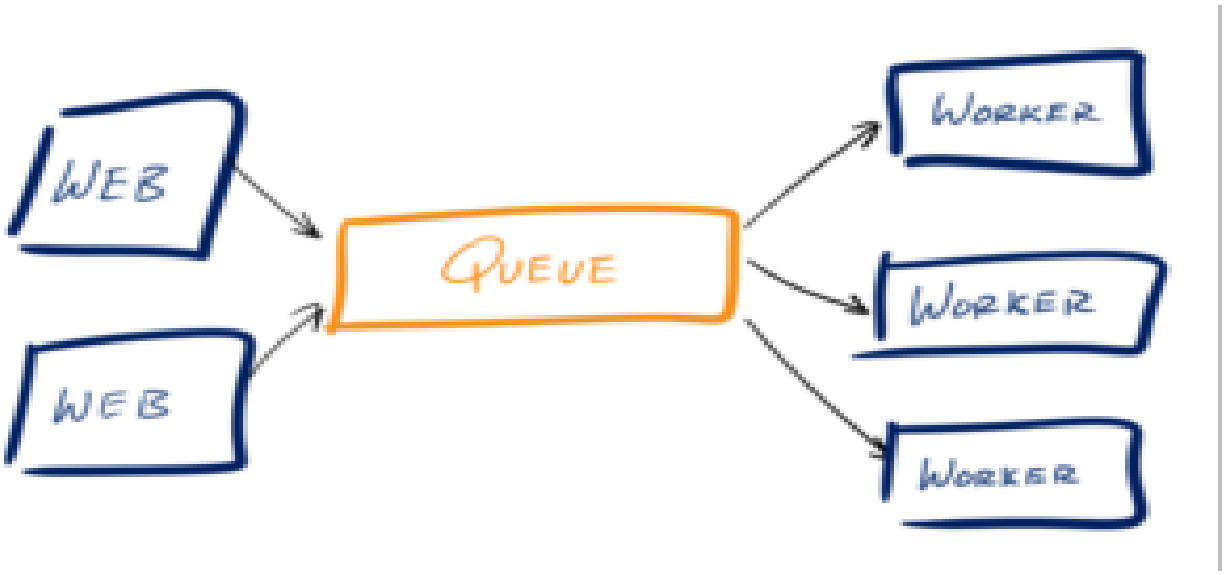


Fig: www. robertgreiner.com

The Worker Role runs alongside with the Web Role and performs the computing functions needed for the smooth operation of your application. The Web Role will accept the user's input and will queue up for an action to process later by the Work Role. Subsequently, this enables the Web Role to be more productive and responsive.

Azure PaaS services

Azure offers five main services of Platform as a Service in which multiple service types host a custom application or business logic for specific use cases:

1. Web apps

These are an abstraction of a Web Server such as IIS and Tomcat that run applications written in mostly in Java, Python,.NET, PHP, Node.js, etc. These are simple to set up and provide a variety of benefits, available 99.9% of the time which is a key benefit.

2. Mobile apps

The back ends of mobile apps can be hosted on the Azure PaaS easily using the SDKs available for all major mobile operating systems of iOS, Android, Windows, etc. It enables the unique ability of offline sync so the user can use the app even if they are

offline and sync the data back when they are back online. Another major benefit is the ability to push notifications allowing sending of custom notifications for all targeted application users.

3. Logic apps

No apps are hosted, but there is an orchestrated business logic app to automate a business process. These are initiated by a trigger when a predefined business condition is met.

4. Functions

Functional apps can perform multiple tasks within the same application. These functional apps host smaller applications such as microservices and background jobs that only run for short periods.

5. Web jobs

These are a part of a service that runs within an app service on web apps or mobile apps. They are similar to Functions but do not require any coding to set it up.

Where PaaS is used?

PaaS is often seen in Business Organizations for the following scenarios:

Development Framework

PaaS offers application developers the ability to create applications using the in-build software components of PaaS such as scalability, multi-tenancy and high availability which highly reduces the amount of coding for the application that the developers must do, making the development life cycle significantly shorter.

Analytics/Business intelligence (BI)

Additional intelligence tools of PaaS allow organizations to mine and analyze both user behavioral data and application data, predict the outcomes to improve the product design decisions, business decisions, and increase the return on investment by analyzing insights and application usage patterns.

Along with the scenarios mentioned earlier, PaaS includes additional services that enable users to have a stable PaaS platform and enhance the applications hosted, like security and workflow scheduling. It allows new capabilities without the need to add additional staff with specific skills to implement these features.

Why use PaaS?

Since PaaS builds on top of IaaS, PaaS offers more features of business tools, middleware and development tools while providing the advantages and value that come up with IaaS.

Time efficiency

With the development tools offered by PaaS, developers can further reduce the time spent for coding the new app since they can integrate the pre-coded components of the platform such as security features, directory services, search options, etc. into the developing application.

Application lifecycle

You can manage Application Lifecycle efficiently because PaaS is designed to support the complete web application lifecycle of building, testing, deploying, managing, and updating.

Multi-platform support

The ability to develop applications for multiple platforms of computers mobile devices and browsers makes application development much easier and quicker.

Geo-distributed development

Since the development environment is accessible via the internet, multiple development teams located in various locations can work together on application development.

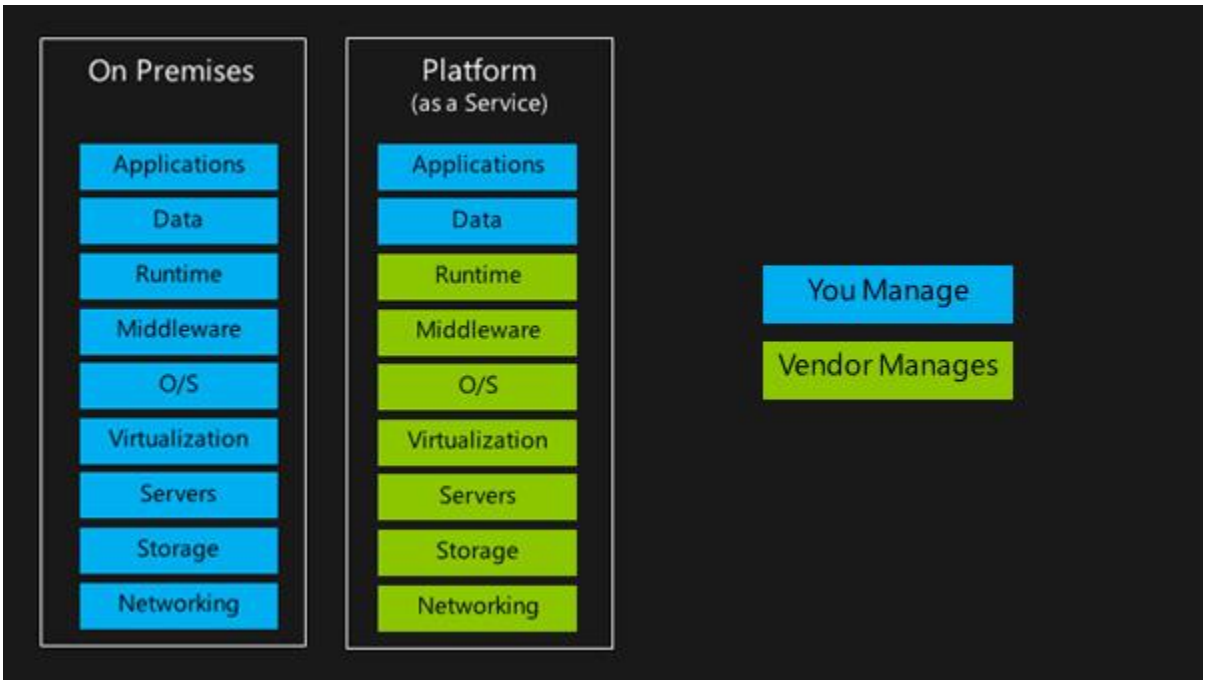
Cost

The primary benefit of using PaaS is its utility billing model, i.e., it bills only for what is used. Because PaaS provides both the hardware and the software infrastructure eliminating the need to invest in hardware and software, it yields significant cost savings.

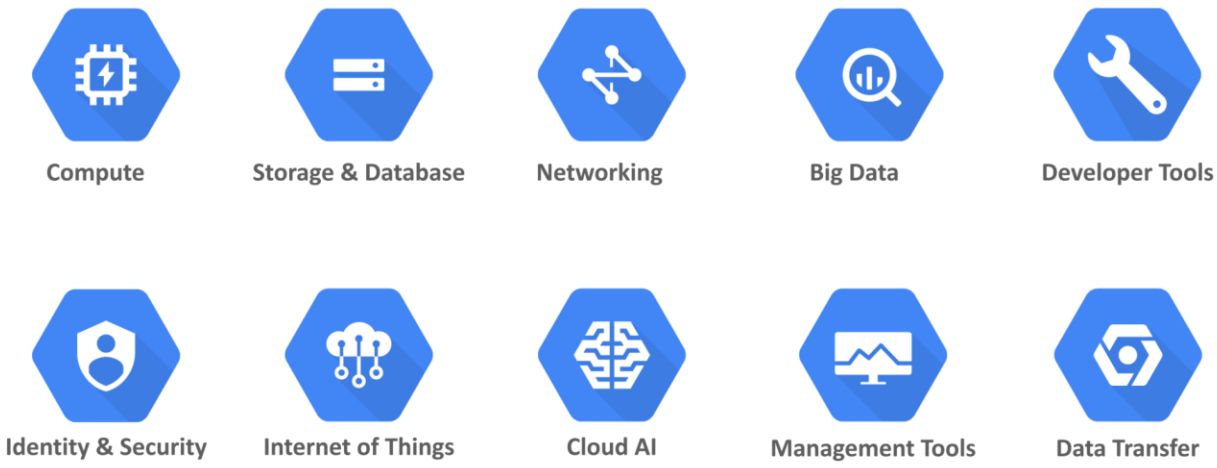
Who is Azure PaaS for?

In General, Azure PaaS is ideal for but not limited to:

- Development teams in businesses who want to significantly reduce the time it takes their applications time to get on the market.
- Organizations that have high operational costs that want to lessen the administration needs for a set of applications.
- Organizations that require critical support metrics for usage and chargeback.
- Organizations that want to slash costs spent on IT, and reduce database elements and operating systems complexity while increasing scalability.
- Businesses that want to improve the quality of service of their company can greatly benefit from PaaS.



Google Cloud Platform as a Service (PAAS)



The primary PaaS services offered by Google Cloud are:

1.Google App Engine — serverless app-hosting in the cloud (web apps, mobile backends, etc.); Google's first cloud product, supports Python, Java, Go, PHP, Node.js, Ruby.

2.Google Cloud Functions — serverless function-hosting in the cloud (for when you don't have an entire app and want to run functions or provide microservices); supports Node.js, Python, Go.

3.Cloud Functions for Firebase — this is a derivative product customized for Firebase, Google's mobile development platform. Whereas you have more access to GCP products from GCF, you have access to more Firebase products from CF4F. Incidentally, DialogFlow fulfillment "handlers" for "Actions on Google" voice-driven apps for the Google Assistant or Home/Nest products are CF4F functions.

4.Google Cloud Run — container-hosting in the cloud for your apps that can't run on higher-level systems like App Engine or Cloud Functions (due to language or library restrictions) where you've containerized your app and want to run it serverlessly and fully-managed. If you have other requirements (HW config, GPUs, VPC, etc.), consider Cloud Run (for Anthos) on Google Kubernetes Engine (GKE) — fully-managed Kubernetes clusters in the cloud.

Google Apps Script is what I refer to as a "restricted PaaS" system. Similar to "force.com", these PaaS systems are generally tied to data that live at the SaaS level (hence why they live in b/w Saas & PaaS). For Apps Script, that would be G Suite/Google Apps data, and Salesforce data for "force.com". Unless you have that type

of data, there's no reason not to use a more generalized, more flexible PaaS system instead.

References

1. **https://magenest.com/en/aws-iaas-paas-saas/**
2. **https://cdn2.hubspot.net/hubfs/1629777/A%20Comprehensive%20Guide%20on%20AWS%20as%20SaaS_IaaS_and_PaaS.pdf**
3. **https://searchcloudcomputing.techtarget.com/tip/IaaS-vs-PaaS-options-on-AWS-Azure-and-Google-Cloud-Platform**
4. **https://www.sherweb.com/blog/cloud-server/what-is-azure-paas/**
5. https://www.edureka.co/blog/what-is-google-cloud-platform/