***CYBER SECURITY***

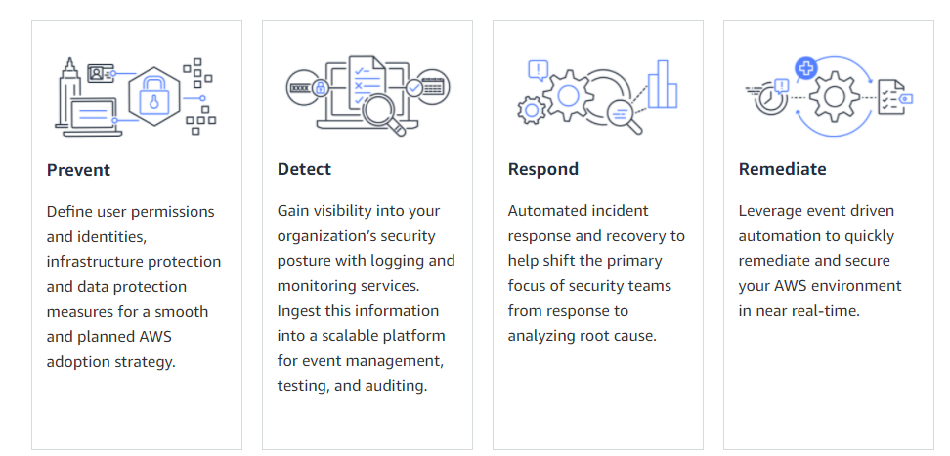
Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

AWS Cloud Security

### **Raise your security posture with AWS infrastructure and services.**

Using AWS, you will gain the control and confidence you need to securely run your business with the most flexible and secure cloud computing environment available today. As an AWS customer, you will benefit from AWS data centers and a network architected to protect your information, identities, applications, and devices. With AWS, you can improve your ability to meet core security and compliance requirements, such as data locality, protection, and confidentiality with our comprehensive services and features.

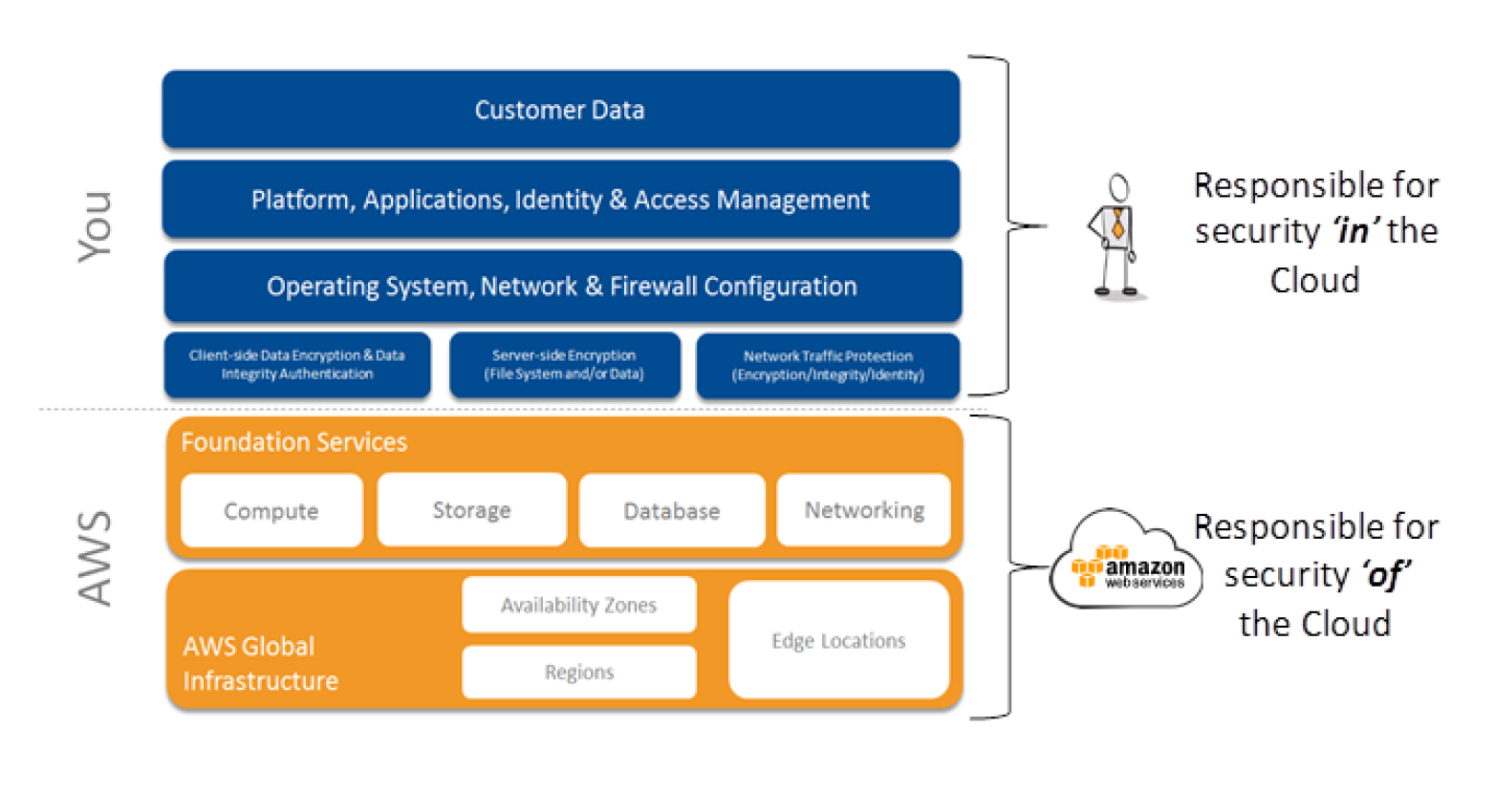
AWS allows you to automate manual security tasks so you can shift your focus to scaling and innovating your business. Plus, you pay only for the services that you use. All customers benefit from AWS being the only commercial cloud that has had its service offerings and associated supply chain vetted and accepted as secure enough for top-secret workloads.



## **Strategic Security**

AWS is designed to help you build secure, high-performing, resilient, and efficient infrastructure for your applications. World-class security experts who monitor our infrastructure also build and maintain our broad selection of innovative security services, which can help you simplify meeting your own security and regulatory

requirements.



What is AWS Security?

<https://www.youtube.com/watch?v=_2HFqANE4gw&t=16s>

# AZURE Cloud Security

Azure Security refers to security tools and capabilities available on Microsoft’s Azure cloud platform. According to Microsoft, the tools for securing its cloud service encompasses “[**a wide variety of physical, infrastructure, and operational controls**](https://azure.microsoft.com/en-us/services/security-center/).”

As a public cloud computing platform, Azure can support multiple programming languages, operating systems, frameworks, and devices. Customers can access Azure’s services and resources, as long as they are connected to the Internet.

### **WHAT IS AZURE SECURITY CENTER?**

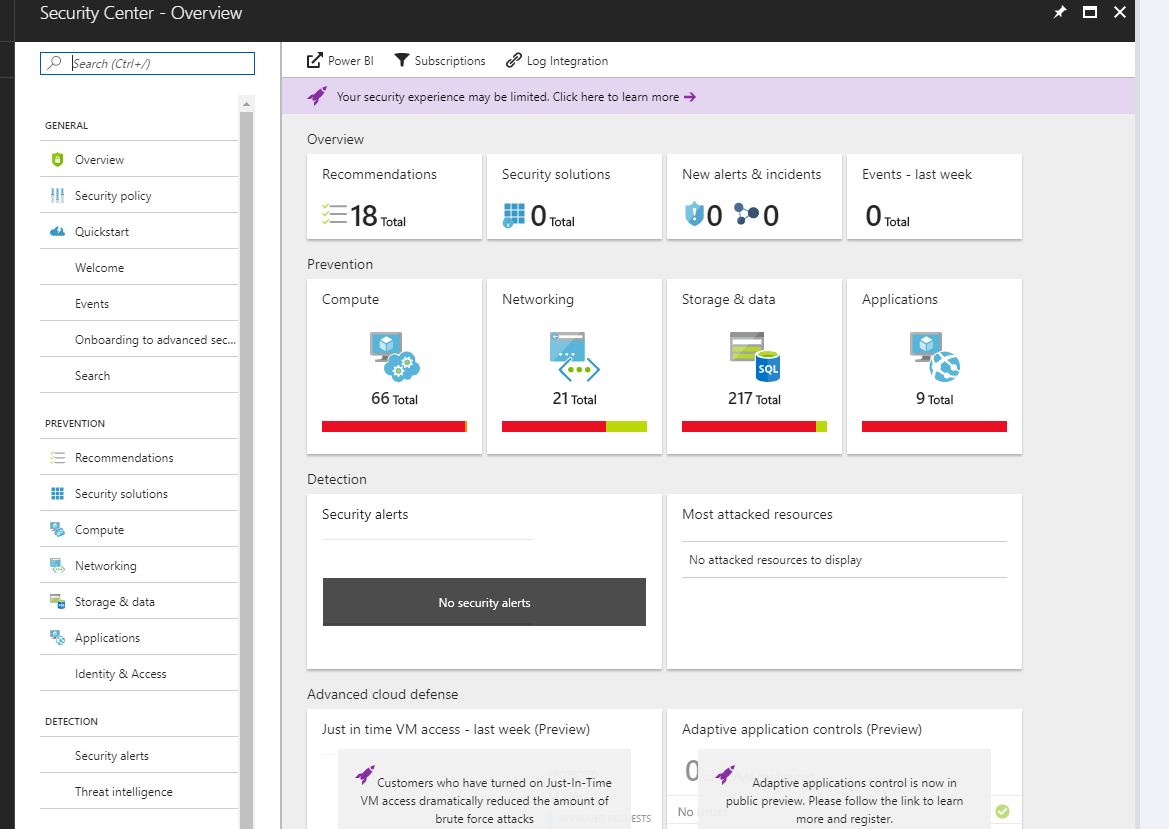
Azure Security Center is a unified security management system offered by Microsoft to Azure customers. Some Azure Security Center benefits customers can enjoy are:

* Providing visibility and control over the security of Azure resources (like Virtual Machines, Cloud Services, Azure Virtual Networks, and Blob Storage).
* Protecting hybrid workloads deployed in Azure or non-Azure environments and on customers’ premises.
* Strengthening security posture. The Azure Security Center checks the cloud environment and helps customers understand the status and security of their resources.
* Detecting and blocking cyber security threats. There’s a single dashboard that provides Azure Security Center alerts and recommendations. This also helps with regulatory compliance as security policies can be streamlined across the [Azure Security Center dashboard](https://www.otava.com/reference/what-is-azure-security-center-and-how-do-i-use-it/).

Moreover, the [**Azure Security Center**](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro/) addresses the following security issues and challenges:

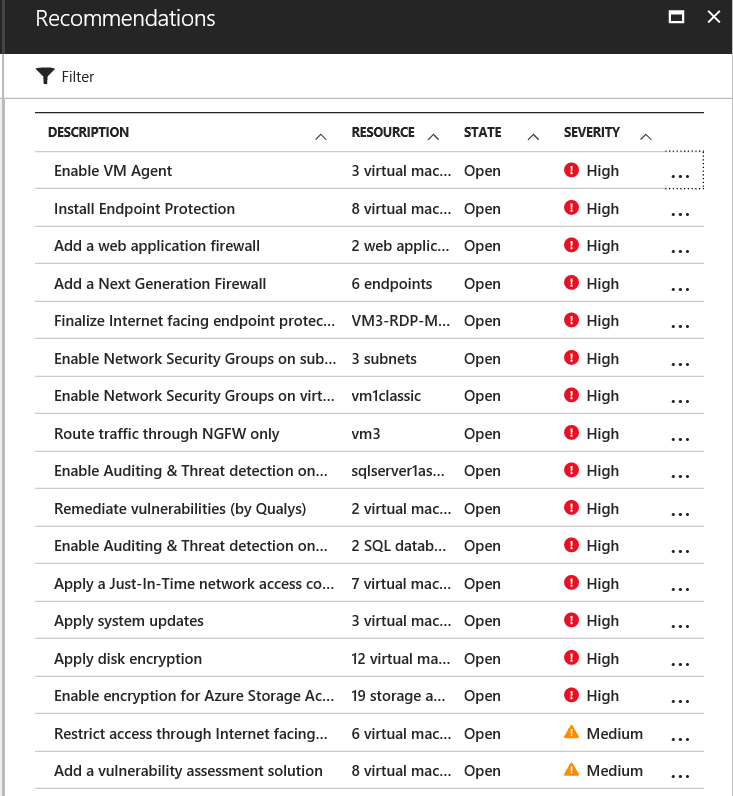
* **Ever-changing workloads:** While customers can do more on the cloud, the services they use change all the time. The Azure Security Center helps in reducing the difficulty of implementing security standards and best practices consistently.
* **Increasingly sophisticated attacks:** As more customers run their workloads on the public cloud, attacks are becoming more sophisticated. Customers must ensure that they also secure their workloads, but doing so could expose them to more vulnerabilities if they don't follow security best practices. Azure Security Center can help take care of that task.
* **Shortage of security skills:** A high number of security alerts and alerting systems can overwhelm administrators, especially if they’re not experienced. But Azure Security Center can help administrators go toe-to-toe with attacks.

When you open the security centre dashboard, you are faced with the ‘Overview’, a summary of the status of your subscriptions, their level of protection, and any recommendations that the security centre might have, in order to tighten security in your cloud network.

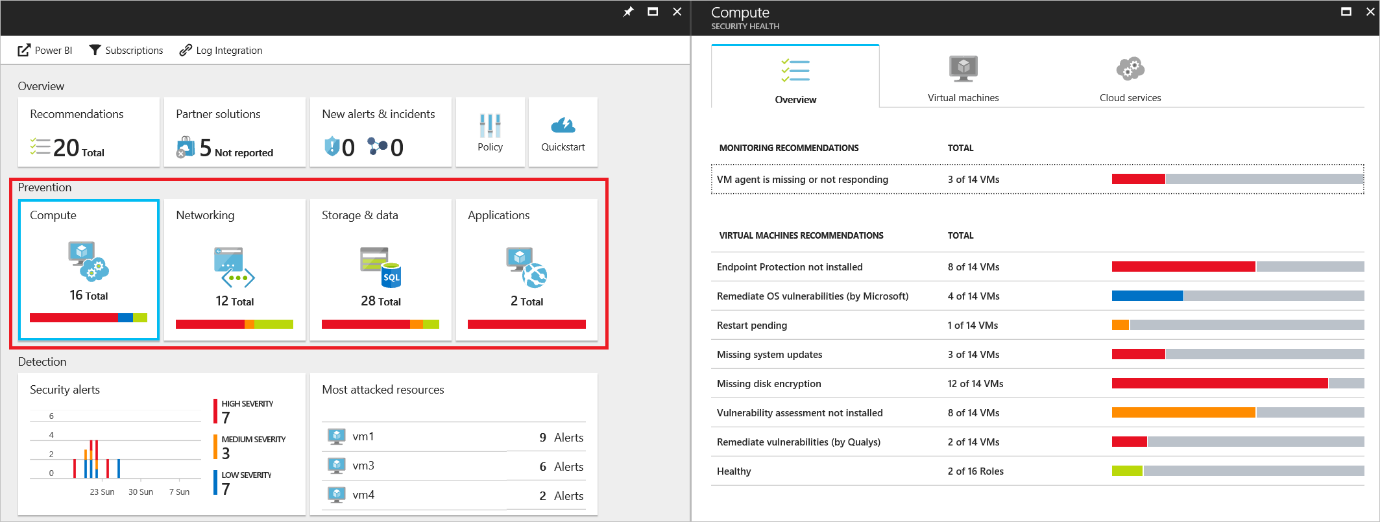


### **CONFIGURE**

Clicking the ‘Recommendations’ tile will list them in a new blade, and you can select each one to view more information about each recommendation and take steps to resolve any issues.



**MONITOR**



Cyber Security in Azure

<https://www.youtube.com/watch?v=mntOLLNejUo>

# Google Cloud Platform Security

Google, which happens to be one of the largest tech companies in the world after Amazon has for years warding off security threats by following certain guidelines in its day to day operations. In the last weekend, the internet juggernaut decided to disclose some security features of its Google Cloud Platform to help customers show their data and services are being offered securely to help build ‘Trust’ among its patrons.

Going by the disclosure it appears that the web search giant has customized most of its cloud security features as per its needs and demands from customers and a summary of it is as follows-

**Google Data Center security on the physical note-** When it comes to the protection of its data center assets, the Alphabet Inc’s subsidiary seems to be very serious. The company is seen protecting its infrastructure with the help of biometric detectors, alarms, cameras, security lasers with minimalistic human indulgence. So, as everything is automated at this segment, errors are almost negligible or mere zero.

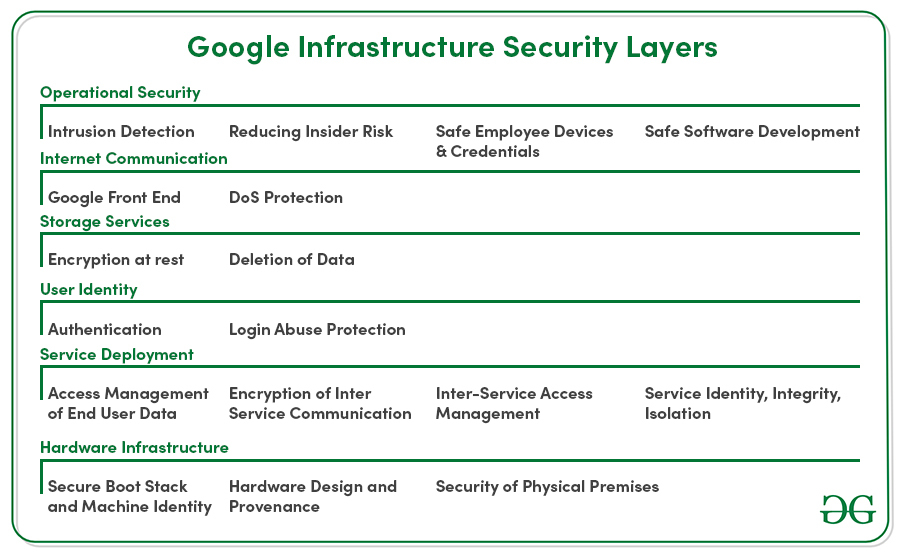
**Highly customized Hardware and Software-** Google has announced to the world in the year 2015 that it builds its hardware like server boards, networking devices, and customized server machines- all as per its needs and security requirements. And when it comes to software’s like firmware stack, curated OS images, and hardened hypervisors are all tuned as per its requirements.

**Data storage and destruction-** As the Sundar Pichai firm happens to have tons of Petabytes of data moving to and fro, at the end of the data it also has to do persistent disk cleanups to make way for the new lot. Google says that data destruction at its premises is done scientifically by using a logical disk cleaning technique for cleanups and the results of erasure are securely stored and logged in the disks in a perfect way for future weekly audits. Then the erased disk is released into the inventory for reuse.

**Data encryption** is also done at two points on GCP. As the encryption is automatic it requires no action from the user’s side. An AES- 256 algorithm is applied with master keys which are again termed by the Google servers.

Network monitoring, data access monitoring, intrusion detention are all kept operational at the server farms of Google. DDoS protection, login abuse protection, and authentication are being given a priority by the tech giant these days.

**Note-** As Mountain View-based company offers different services, the above-specified security standards are being followed to render services related to Gmail, Google Search, Google Photos, and other enterprise services like G-Suite and GCP.

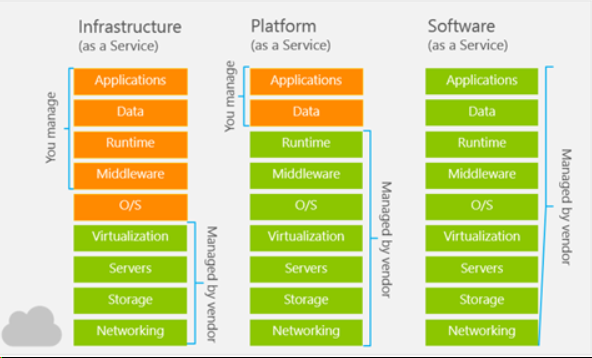


**Security in GCP**

<https://www.youtube.com/watch?v=UOdUC8DhprQ>

***Platform-as-a-Service***

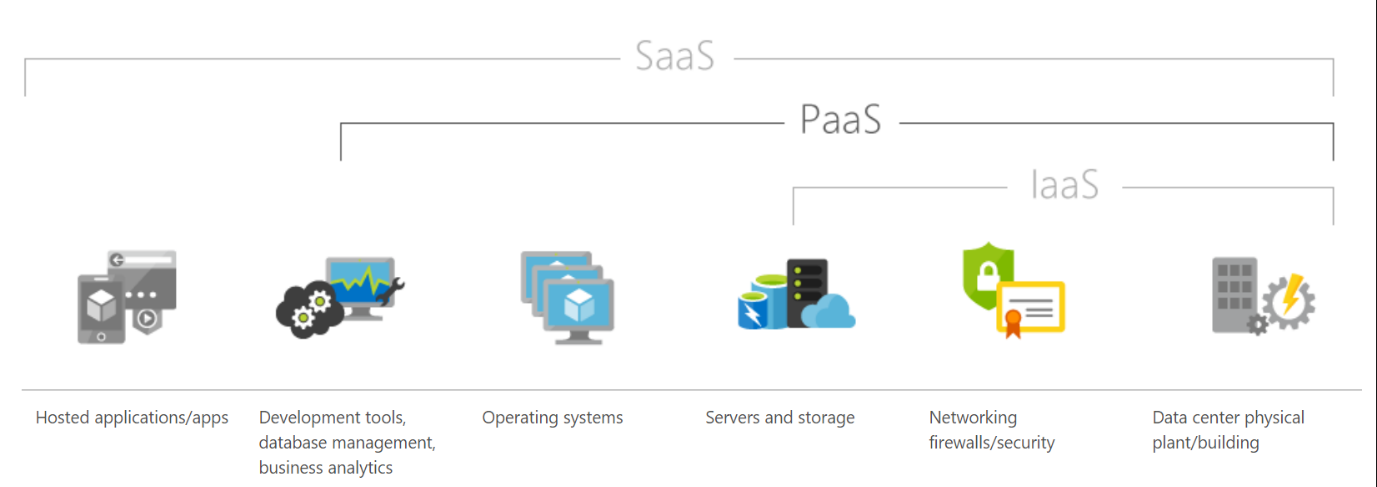
**What is Microsoft Azure Platform-as-a-Service (PaaS)?**



## **Azure Platform-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.



## **Azure PaaS services**

Azure offers five main services of Platform as a Service in which multiple service types host a custom application or a 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.

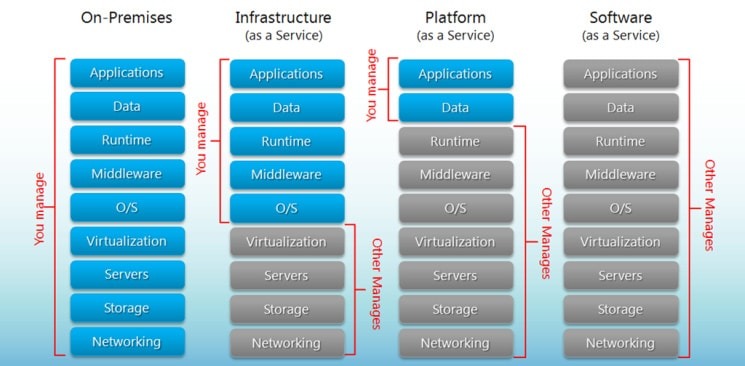
## **Who is Azure PaaS for?**

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.

**What is AWS as Platform-as-a-Service (PaaS)?**

* Platforms 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.



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

### **PaaS (Platform as a Service).**

A PaaS vendor provides hardware and software tools over the internet, and people use these tools to develop applications. PaaS users tend to be developers.

#### **PaaS Characteristics:**

PaaS platforms are:

* Accessible by multiple users.
* Scalable – you can choose from various tiers of resources to suit the size of your business.
* Built on virtualization technology.
* Easy to run without extensive system administration knowledge.

#### **When to Use PaaS:**

PaaS is often the most cost-effective and time-effective way for a developer to create a unique application.

PaaS allows the developer to focus on the creative side of app development, as opposed to menial tasks such as managing software updates or security patches. All of their time and brainpower will go into creating, testing, and deploying the app.

#### **PaaS Non-Ecommerce Example:**

A good example of PaaS is [AWS Elastic Beanstalk](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html).

Amazon Web Services (AWS) offers over 100 cloud computing services such as EC2, RDS, and S3.

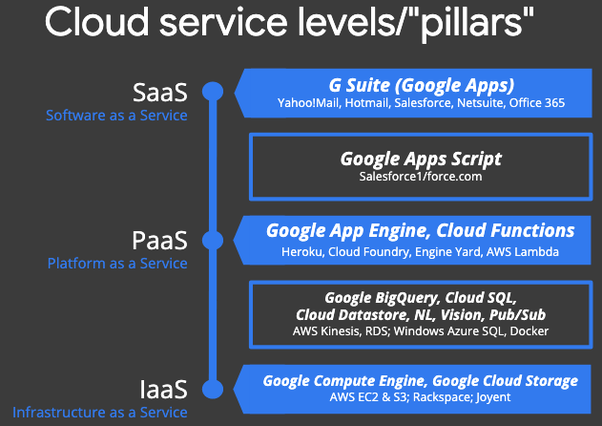
Most of these services can be used as IaaS, and most companies who use AWS will pick and choose the services they need.

However, managing multiple different services can quickly become difficult and time-consuming for users.

**What is GCP as Platform-as-a-Service (PaaS)?**

These are some **PaaS services offered by Google Cloud**:

* Google App Engine which is an application platform for apps and back ends. With it, Google handles most of the management of the resources for you.
* Apigee API Management, which helps leading companies design, secure, and scale application programming interfaces (APIs).
* BigQuery, which is a fully-managed, serverless data warehouse that enables scalable analysis over huge amounts of data.
* Google Maps, for adding location intelligence to your operations.
* Google Kubernetes Engine (GKE), which is a managed, production-ready environment for running containerized applications.



The primary PaaS services offered by Google Cloud are:

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.

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.

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.

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.

There are no other Google products that fall under “PaaS” services at the time of this writing.

**Reference:**

<https://digitalguardian.com/blog/what-azure-security>

<https://aviatrix.com/learn-center/cloud-security/network-security-azure/>

<https://www.xenonstack.com/blog/google-security-services>

<https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf>

<https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf>

<https://www.quora.com/Which-are-the-PaaS-services-offered-by-Google-Cloud>

<https://azure.microsoft.com/en-in/overview/what-is-paas/>

<https://www.sherweb.com/blog/cloud-server/what-is-azure-paas/>

<https://magenest.com/en/aws-iaas-paas-saas/>