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.

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.

**The scale of the cyber threat**

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

Medical services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

With the scale of the cyber threat set to continue to rise, the International Data Corporation predicts that worldwide spending on cyber-security solutions will reach a massive $133.7 billion by 2022. Governments across the globe have responded to the rising cyber threat with guidance to help organizations implement effective cyber-security practices.

In the U.S., the National Institute of Standards and Technology (NIST) has created a cyber-security framework. To combat the proliferation of malicious code and aid in early detection, the framework recommends continuous, real-time monitoring of all electronic resources.

The importance of system monitoring is echoed in the “10 steps to cyber security”, guidance provided by the U.K. government’s National Cyber Security Centre. In Australia, The Australian Cyber Security Centre(ACSC) regularly publishes guidance on how organizations can counter the latest cyber-security threats.



Types of cyber threats

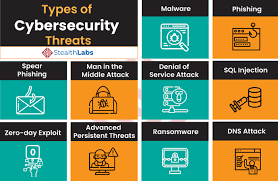
The threats countered by cyber-security are three-fold:

1. Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

2. Cyber-attack often involves politically motivated information gathering.

3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:



Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

·Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

·Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

·Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

·Ransomware: Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

·Adware: Advertising software which can be used to spread malware.

·Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.’s National Cyber Security Centre advises the public to “ensure devices are patched, anti-virus is turned on and up to date and files are backed up”.

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and are designed to encrypt or wipe data from computer’s hard drive.

Electronic security protocols also focus on real-time malware detection. Many use heuristic and behavioural analysis to monitor the behaviour of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyze their behavior and learn how to better detect new infections.

Security programs continue to evolve new defenses as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1.Update your software and operating system: This means you benefit from the latest security patches.

2.Use anti-virus software: Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.

3.Use strong passwords: Ensure your passwords are not easily guessable.

4.Do not open email attachments from unknown senders: These could be infected with malware.

5.Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.

6.Avoid using unsecure WIFI networks in public places: Unsecure networks leave you vulnerable to man in the middle attacks.



CYBER SECURITY IN MICROSOFT AZURE :

Azure Security refers to security tools and capabilities available on Microsoft’s Azure cloud platform. In this article, we’ll discuss Azure Security and the Azure Security Center.

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.”

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.

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.

Moreover, the Azure Security Center 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.

Azure Security documentation shows that Microsoft Azure Security infrastructure operates under a shared security responsibility model. This means security is a joint effort between Azure and the customers, except in an on-premise setting where the customers carry all the responsibilities.



However, as customers move into the cloud, some Azure customer security responsibilities are transferred.

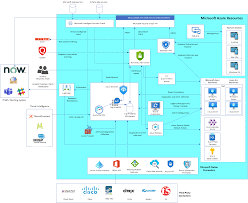
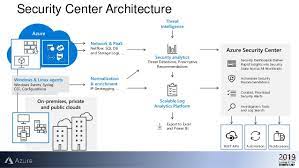
This is how the division of responsibilities changes across different cloud service models:

•In IaaS (infrastructure as a service), Azure takes over physical security (hosts, networks, and data center).

•In PaaS (platform as a service), Azure takes over physical security and the operating system. Azure shares identity and directory infrastructure, network controls, and applications with the customers.

•In SaaS (software as a service), Azure takes more responsibilities: physical security, operating system, network controls, and application. Azure would still share identity and directory infrastructure with the customer.

In a nutshell, Azure secures the physical infrastructure, then the division of responsibilities changes depending on the cloud delivery model. Customers have more responsibilities in IaaS than in PaaS or SaaS. Regardless of whether it’s on-premise, IaaS, PaaS, or SaaS, customers are always be responsible for these three aspects: data governance and rights management, account and access management, and endpoint protection.

AZURE SECURITY BEST PRACTICES

The Azure Security documentation is also a handy source for security recommendations and best practices. Here are some tips to get you started quickly:

•Upgrade your Azure subscription to Azure Security Center Standard to enjoy more functionality, like finding and fixing security vulnerabilities, detecting threats with analytics and intelligence, and quick response to an attack.

•Store your keys in the Azure Key Vault. This vault is designed to support passwords, database credentials, and other secrets.

•Install a web application firewall.

•Use Azure MFA (Multi-factor Authentication), especially for admin accounts.

•Encrypt virtual hard disk files.

•Connect Azure VMs (virtual machines) to other networked devices by placing them on Azure virtual networks.

•Use Azure’s DDoS services to prevent and mitigate DDoS (distributed denial of service) attacks.

•Have security policies in place to prevent abuse. To help you get started, Azure can auto-generate a security policy per an Azure subscription.

•Regularly review the Azure Security Center dashboard. The dashboard provides a central view of your Azure resources and recommends actions.

•Implement Azure Security Center’s Role-Based Access Control (RBAC). There are five built-in roles (Subscription Owner, Resource Group Owner, Subscription Contributor, Resource Group Contributor, and Reader) and two unique security roles (Security Administrator and Security Reader). These roles vary in permissions.

AWS

Raise your security posture with AWS infrastructure and services.

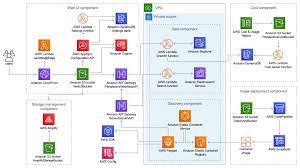
Using AWS, you will gain the control and confidence you need to securely run your business with the most flexible and secure cloud computing environment available today. As an AWS customer, you will benefit from AWS data center and a network architected to protect your information, identities, applications, 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.









Benefits

Scale Securely with Superior Visibility and Control

With AWS, you control where your data is stored, who can access it, and what resources your organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information ensures that the right resources have the right access at all times, wherever your information is stored. Reduce risk as you scale by using our security automation and activity monitoring services to detect suspicious security events, like configuration changes, across your ecosystem. You can even integrate our services with your existing solutions to support existing workflows, streamline your operations, and simplify compliance reporting.

Automate and Reduce Risk with Deeply Integrated Services

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work critical to your business. Select from a wide variety of deeply integrated solutions that can be combined to automate tasks in novel ways, making it easier for your security team to work closely with developer and operations teams to create and deploy code faster and more securely. For example, by employing technologies like machine learning, AWS enables you to automatically and continuously discover, classify, and protect sensitive data in AWS with just a few clicks in the AWS console. You can also automate infrastructure and application security checks to continually enforce your security and compliance controls and help ensure confidentiality, integrity, and availability at all times. Automate in a hybrid environment with our information management and security tools to easily integrate AWS as a seamless and secure extension of your on-premises and legacy environments.

Build with the Highest Standards for Privacy and Data Security

AWS is vigilant about your privacy. Because our customers care deeply about data security, we have a world-class team of security experts monitoring our systems 24x7 to protect your content. With AWS you can build on the most secure global infrastructure, knowing you always own your data, including the ability to encrypt it, move it, and manage retention. All data flowing across the AWS global network that interconnects our data centers and regions is automatically encrypted at the physical layer before it leaves our secured facilities. Additional encryption layers exist as well; for example, all VPC cross-region peering traffic, and customer or service-to-service TLS connections. We provide tools that allow you to easily encrypt your data in transit and at rest to help ensure that only authorized users can access it, using keys managed by our AWS Key Management System (KMS) or managing your own encryption keys with Cloud HSM using FIPS 140-2 Level 3 validated HSMs. We also give you the control and visibility you need to help demonstrate that you comply with regional and local data privacy laws and regulations. The design of our global infrastructure allows you to retain complete control over the regions in which your data is physically located, helping you meet data residency requirements.

Largest Ecosystem of Security Partners and Solutions

Extend the benefits of AWS by using security technology and consulting services from familiar solution providers you already know and trust. We have carefully selected providers with deep expertise and proven success securing every stage of cloud adoption, from initial migration through ongoing day to day management. Choose from our AWS Partner Network (APN), a global program of Technology and Consulting Partners many of whom specialize in delivering security-focused solutions and services for your specific workloads and use cases. APN Partner solutions enable automation and agility and scaling with your workloads. Easily find, buy, deploy, and manage these cloud-ready software solutions, including software as a service (SaaS) products, in a matter of minutes from AWS Marketplace. These solutions work together to help secure your data in ways not possible on-premises, with solutions available for a wide range of workloads and use cases.

Inherit the Most Comprehensive Security and Compliance Controls

To aid your compliance efforts, AWS regularly achieves third-party validation for thousands of global compliance requirements that we continually monitor to help you meet security and compliance standards for finance, retail, healthcare, government, and beyond. You inherit the latest security controls operated by AWS, strengthening your own compliance and certification programs, while also receiving access to tools you can use to reduce your cost and time to run your own specific security assurance requirements. AWS supports more security standards and compliance certifications than any other offering, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping satisfy compliance requirements for virtually every regulatory agency around the globe.

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. Our security services and solutions are focused on delivering the following key strategic benefits critical to helping you implement your organization’s optimal security posture:

Prevent

Define user permissions and identities, infrastructure protection and data protection measures for a smooth and planned AWS adoption strategy.

Detect

Gain visibility into your organization’s security posture with logging and monitoring services. Ingest this information into a scalable platform for event management, testing, and auditing.

Respond

Automated incident response and recovery to help shift the primary focus of security teams from response to analyzing root cause.

Remediate

Leverage event driven automation to quickly remediate and secure your AWS environment in near real-time

Amazon Web Services (AWS) and Microsoft Azure are the top cloud players.

Let’s take a tour of the comparison of cloud security for AWS and Azure

The most critical doubt that holds back many enterprises from arriving at the decision to move to the cloud is security.

However, the security infrastructure on public cloud platforms such as AWS and Microsoft Azure provides the assurance

for safeguarding sensitive data of enterprises.

As the adoption of cloud computing increases, the emphasis on cloud security is increasing prominently.

In addition, the debate on AWS Security vs Azure Security is a major concern that determines the difference between the two public cloud platforms.

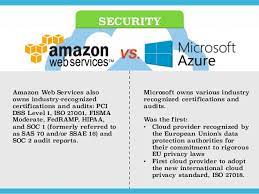
It is highly essential to compare the security infrastructure of both the prominent public cloud service providers.

The comparison can help in finding the ideal cloud platform that aligns with your cloud security requirements.

AWS Security vs Azure Security

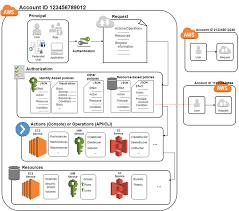
The comparison of AWS Security vs Azure Security should primarily focus only on the services in different aspects of cloud security.

The noticeable areas to consider for the comparison of AWS vs Azure services in terms of security are identity and access management, key-based data encryption, storage data encryption, virtual private network, and monitoring.

Identity and Access Management

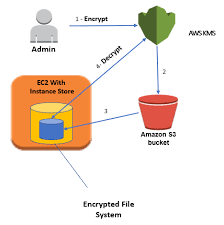
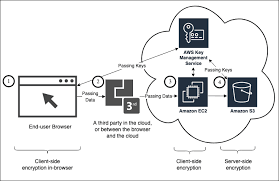
Identity and access management is a significant aspect of cloud security from a customer’s perspective. However, Azure cloud security and AWS cloud security have completely different approaches to identity and access management. Microsoft has extended its legacy identity manager, the Active Directory, from Windows to Azure. The Azure AD comes with a free tier having certain data limits and three distinct paid tiers.



The paid tiers of Azure AD accompany advanced features such as abilities for the management of hybrid environments. On the other hand, AWS offers cloud-centric IAM exclusively without incurring additional charges. The in-built IAM in AWS supports the effective management of cloud environments. However, it has to integrate with other on-premises tools such as Active Directory for achieving its functionality.

Key-Based Data Encryption

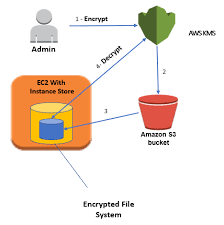
The AWS Security vs Azure Security comparison in terms of key-based data encryptions brings Amazon KMS and Azure Key Vault into question. Both these tools offer data encryption at rest as well as in transit. In addition, both tools can also support key management. However, you would need total control over the encryption and management of keys in certain cases.

You can respond to such cases with the help of a Hardware Security Module (HSM). In the case of Azure, you can find the HSM in-built with Key Vault. On the other hand, the KMS service and Cloud HSM service are separate on AWS. The positive side in this aspect is that pricing is almost similar on both Azure and AWS.

Encryption of Storage Data

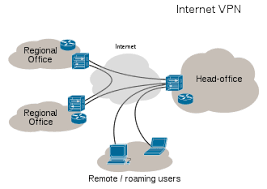
Another important aspect of cloud security comparison is the encryption of stored data. Object data encryption is a very critical component of cloud security and is a profound determinant in the selection of a cloud platform. The Simple Storage Service (S3) on AWS and Blob on Azure provide the cloud storage services and support encryption of data with keys.



Azure doesn’t have support for allowing customers to manage keys although the feature would arrive soon. On the other hand, AWS provides the exclusive option for allowing AWS to manage your keys or choose to manage your keys personally. Therefore, AWS definitely presents better control over cloud security in comparison to Azure for storage data encryption.

Virtual Private Network (VPN)

The importance of Virtual Private Network (VPN) in the AWS Security vs Azure Security comparison is evident due to its role in data encryption. VPN is an ideal instrument for access a private network for data transfer between a public cloud and a data centre. The virtual private network ensures encryption of data as it moves across the internet, thereby offering exceptional data security.



AWS Virtual Private Cloud (VPC) and Direct Connect are the two services to enable virtual private networks. On the other hand, Azure has two similar services such as ExpressRoute and Virtual Network, for creating a VPN. The difference between AWS and Azure Security in this aspect is that AWS uses layer 2 routings while Azure uses layer 3 routings.

Monitoring

Monitoring is a highly critical tool for enforcing security in the cloud. Cloud security has to focus on cloud services as well as the applications they support. AWS CloudWatch provides the monitoring functionality to enforce cloud security. CloudWatch ensures integration of services and application monitoring.

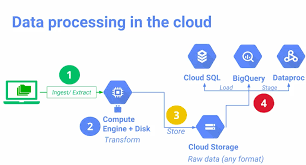


On the other hand, Azure Monitor provides services monitoring and application monitoring distinctively. Azure Monitor can track all Azure services while Azure Application Insights can monitor running applications. The features offered by Azure and AWS in terms of monitoring are almost similar, although with a difference in the organization of features.

**Google Cloud Platform (GCP) Security Fundamentals**

Google Cloud Platform (GCP) security fundamentals include having disaster recovery plans, having high visibility of the environment, monitoring logs of cloud activity, using identity access management (IAM) tools, utilizing automated services, and encrypting data at all times.

As with any public [cloud provider](https://www.sdxcentral.com/cloud/definitions/what-are-cloud-service-providers/), there are aspects of [the cloud](https://www.sdxcentral.com/cloud/definitions/what-is-cloud/) environment that the customer is responsible for and aspects the provider is responsible for. The shared responsibility varies between different service models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The following image shows the different responsibilities.



## Have a Plan for Security Events and Recovery

It is a best practice for an organization to have a plan for how to prevent, detect, and respond to a security breach. When an organization experiences a security event, it needs to be prepared with a disaster recovery plan to mitigate the damage and recover from whatever data it may lose in the process.

The [GCP security](https://www.sdxcentral.com/cloud/definitions/cloud-security-basics-definition/) documentation has a guide for how to plan for[disaster recovery here](https://cloud.google.com/solutions/dr-scenarios-planning-guide).

## Ensure High Visibility and Monitor the Cloud Environment

An organization needs visibility over every corner of its cloud environment to effectively mitigate security. Using services that enhance visibility into the environment allows organizations to detect attacks faster and with more precision. Key parts in this include actively monitoring logs to detect anomalous behaviour and automation.

GCP’s[Security Command Center](https://cloud.google.com/security-command-center) is designed for this purpose. It can identify misconfigured security functions in virtual machines (VMs), networks, applications, and [storage](https://www.sdxcentral.com/data-center/storage/definitions/what-is-software-defined-storage/) buckets. The [Security](https://www.sdxcentral.com/security/definitions/what-is-software-defined-security/) Command Center monitors security logs to detect compromised VMs. It also provides recommendations to the administrators using the dashboard.

The[Cloud Monitoring](https://cloud.google.com/monitoring) service from GCP collects metrics, events, and metadata from both GCP and AWS, along with hosted uptime probes, application instrumentation, and several other application components. The information is collected automatically. Cloud Monitoring also creates insights based on the information, which alert administrators and presents visual representations of its findings. It also looks at patterns and anomalies to determine long-term trends.

Both of these services enable organizations to be more aware of what is happening in their cloud and what to do when an incident occurs.

## Utilize Identity Access Management

The principle of least privilege is a critical foundational element in GCP security and security more broadly. The principle is the concept of only providing employees with access to applications and resources they need to properly do their [jobs](https://www.sdxcentral.com/industry/career/digital-transformation/5-tips-for-your-next-tech-job-search/). For example, G Suite administrators can control[how employees share files and folders](https://support.google.com/a/answer/60781?hl=en) in Google Drive. In GCP, administrators can take advantage of identity management and context-aware access tools to limit employee access to the cloud.

[Cloud Identity and Access Management](https://cloud.google.com/iam) (Cloud IAM) allows administrators to authorize what actions an employee can take on specific cloud resources. Managing resource permissions with Cloud IAM is highly automated. When roles for individuals and groups are established, applying the roles does not have to be done manually, but rather[can be done programmatically](https://cloud.google.com/iam/docs/granting-changing-revoking-access#programmatic) using a command-line tool, the REST API, or client libraries. This helps organizations keep their employees from accidentally manipulating resources or seeing confidential information they shouldn’t.

A virtual private cloud (VPC) creates a secure perimeter around cloud resources. Essentially, it creates a cloud environment within a public cloud that a limited number of users can access.[VPC Service Controls](https://cloud.google.com/vpc-service-controls) from GCP is a service that does just that. VPC Service Controls provides context-aware access that allows administrators to create more detailed access control policies. User attributes like user identity and IP address can be used by administrators as criteria for whether a user or group can have access to cloud resources. Organizations with especially sensitive information or who to closely limit who can manipulate cloud resources can benefit from VPC Service Controls.

## Use Automation to Accelerate GCP Security Measures

[Automation](https://www.sdxcentral.com/networking/virtualization/definitions/what-is-network-automation-with-network-virtualization/) is a feature included in some services mentioned above. It is important because cloud environments can quickly become complex. When traffic and data generation increase sharply over a short period of time, the cloud is forced to scale up in response. For example, with Cyber Monday sending immense amounts of customers to a retailer’s website, cloud resources must scale to keep up to keep the site running.

When an organization’s cloud environment grows, administrators suddenly have more to monitor and protect. Automation is key to giving responsibility for monotonous and time-consuming tasks to software, allowing administrators to keep an eye on the overall cloud environment and having more impact on [cloud security](https://www.sdxcentral.com/cloud/definitions/cloud-security-basics-definition/).

## Encrypt Data as a Baseline

If an attacker manages to get access to unencrypted data, there’s nothing stopping them from being able to read it. By encrypting data at rest and in transit, data becomes illegible to attackers, who then would need to spend considerable time and compute resources to decrypt the information.

Data in transit is data that is being transmitted over the network to get to where it is needed. Data at rest is data residing in storage ready to be accessed by permitted users.

However, it is also important to secure the cryptographic keys that lock and unlock the encrypted data. Otherwise, if the attackers can get to the keys, then the encryption is effectively meaningless.

Organizations can use GCP security services such as Application-Level Security to encrypt data in transit and Cloud HSM to secure cryptographic keys. For data at rest, a[GCP page states](https://cloud.google.com/security/encryption-at-rest) it “is encrypted by default in all Google Cloud Platform products.”

GCP’s[Application-Level Security](https://cloud.google.com/security/encryption-in-transit/application-layer-transport-security#application-level_security_and_alts) uses Google’s Application Layer Transport Security (ATLS) system. ATLS uses mutual authentication and transport encryption and runs at the network’s application layer. Mutual authentication, or two-way authentication, is when the sending and receiving parties authenticate each other at the same time. It protects Remote Procedure Calls (RPC) with these steps.

Hardware security modules (HSMs) are physical devices that host encryption keys and execute cryptographic functions.[Cloud HSM](https://cloud.google.com/hsm) is the GCP security service that protects these keys. In Cloud HSM, the devices meet requirements set by[FIPS 140-2 Level 3](https://www.sdxcentral.com/security/definitions/what-does-mean-fips-compliant/), a certification created by the United States government for cryptographic modules.

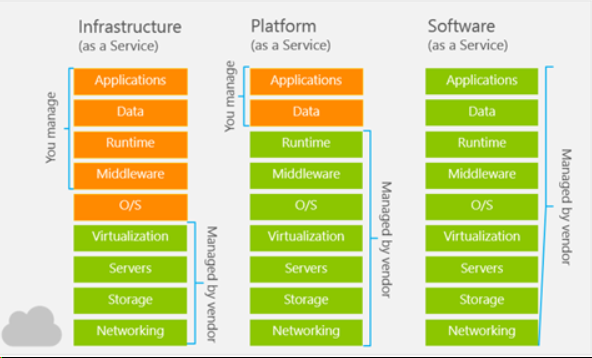
If an organization wants to create, use, rotate, and destroy various cryptographic keys itself, then the[Cloud Key Management Service](https://cloud.google.com/kms) (KMS) is the service to use. This service from GCP is integrated with Cloud IAM and[Cloud Audit Logs](https://cloud.google.com/logging/docs/audit) for easier management. Permissions for specific keys can be managed and their use monitored. Automation can be applied to rotate keys regularly. Symmetric and asymmetric keys can be used so organizations can have the type of encryption they want.



## GCP Security: Key Takeaways

1. Organizations should plan out what they need from their cloud environment and what security services they need to sufficiently protect the environment.
2. Visibility is a key factor in security and is aided by automated monitoring of cloud logs.
3. The principle of least privilege permits employees to only access the resources and applications they need for their job.
4. Identity access management tools enforce the principle of least privilege.
5. Automation streamlines security practices.
6. Data encryption is a must-have to protect data at rest and in transit.

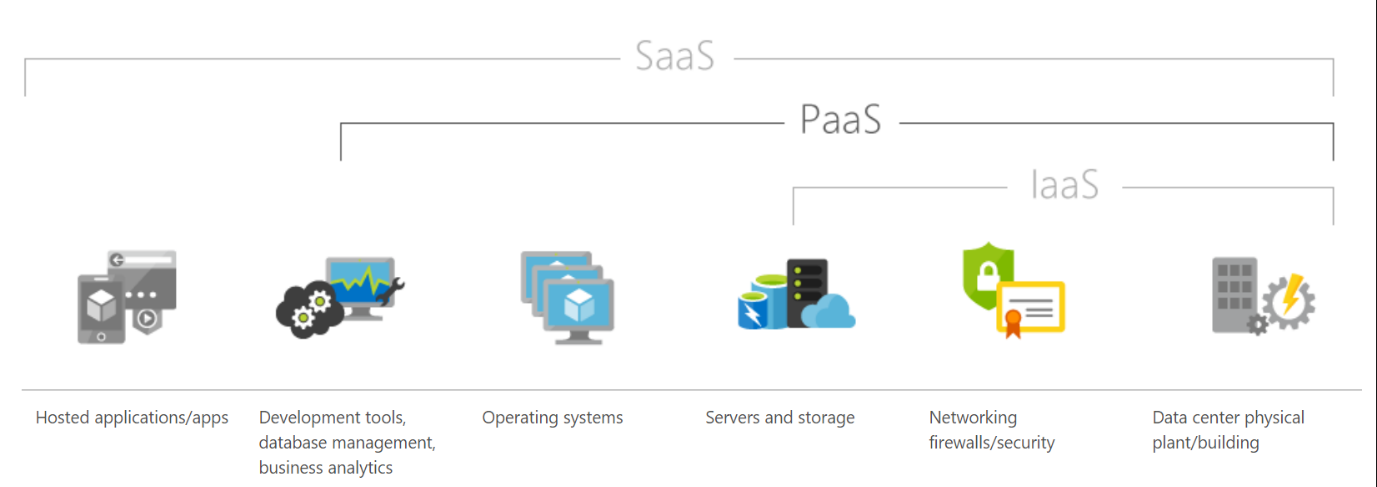
**Microsoft Azure Platform-as-a-Service (PaaS)**



## 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.

PaaS

PaaS is often seen in Business Organizations for the following scenarios

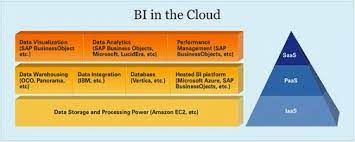
Development Framework

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.

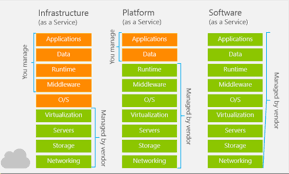
### Cost

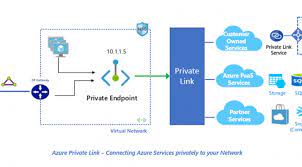
The primary benefit of using PaaS is its utility billing model, i.e., it bills only for what is used. Because PaaS provides both the hardware and the software infrastructure eliminating the need to invest in hardware and software, it yields significant cost savings.

## Who is Azure PaaS for?

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

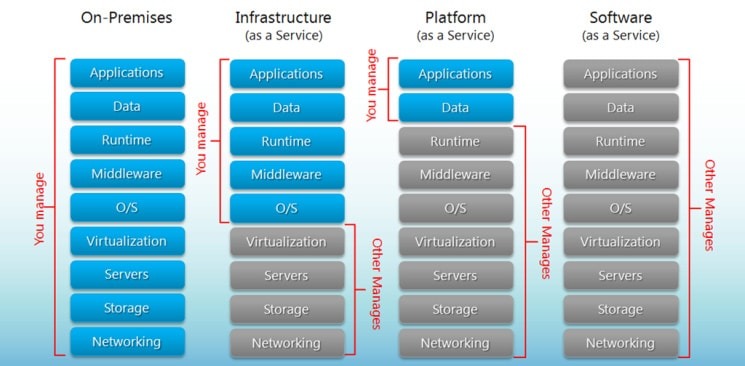
* Development teams in businesses who want to significantly reduce the time it takes their applications time to get on the market.
* Organizations that have high operational costs that want to lessen the administration needs for a set of applications.
* Organizations that require critical support metrics 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.



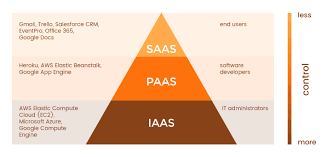


**AWS as Platform-as-a-Service (PaaS)**

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.

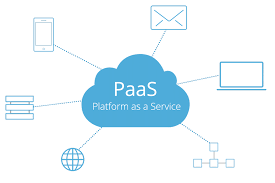


**PaaS examples:**AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.



### 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 Delivery:**

Over the internet.

**PaaS Advantages:**

PaaS is primarily used by developers who are building software or applications.

A PaaS solution provides the platform for developers to create unique, customizable software.

This means developers don’t need to start from scratch when creating applications, saving them a lot of time (and money) on writing extensive code.

PaaS is a popular choice for businesses who want to create unique applications without spending a fortune or taking on all the responsibility.

It’s kind of like the difference between hiring a venue to put on a show vs. building a venue to put on a show.

The venue stays the same, but what you create in that space is unique.

**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.

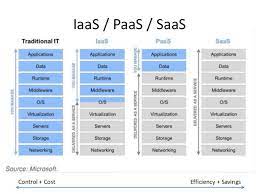
Most of these services can be used as IaaS, and most companies who use AWS will pick and choose the services they need.

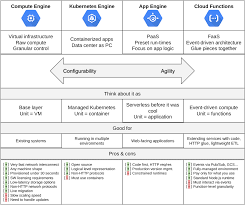
However, managing multiple different services can quickly become difficult and time-consuming for users.

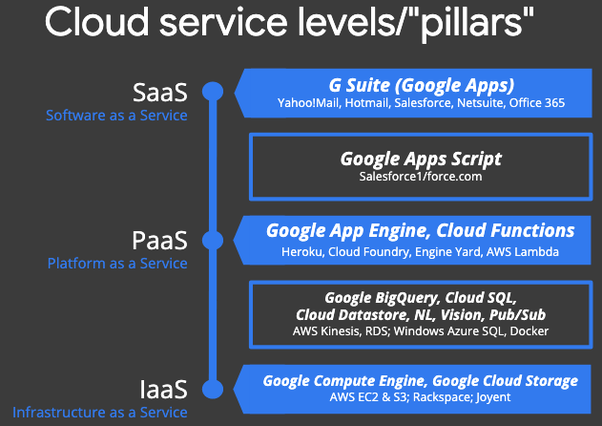
**GCP as Platform-as-a-Service (PaaS)**

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.