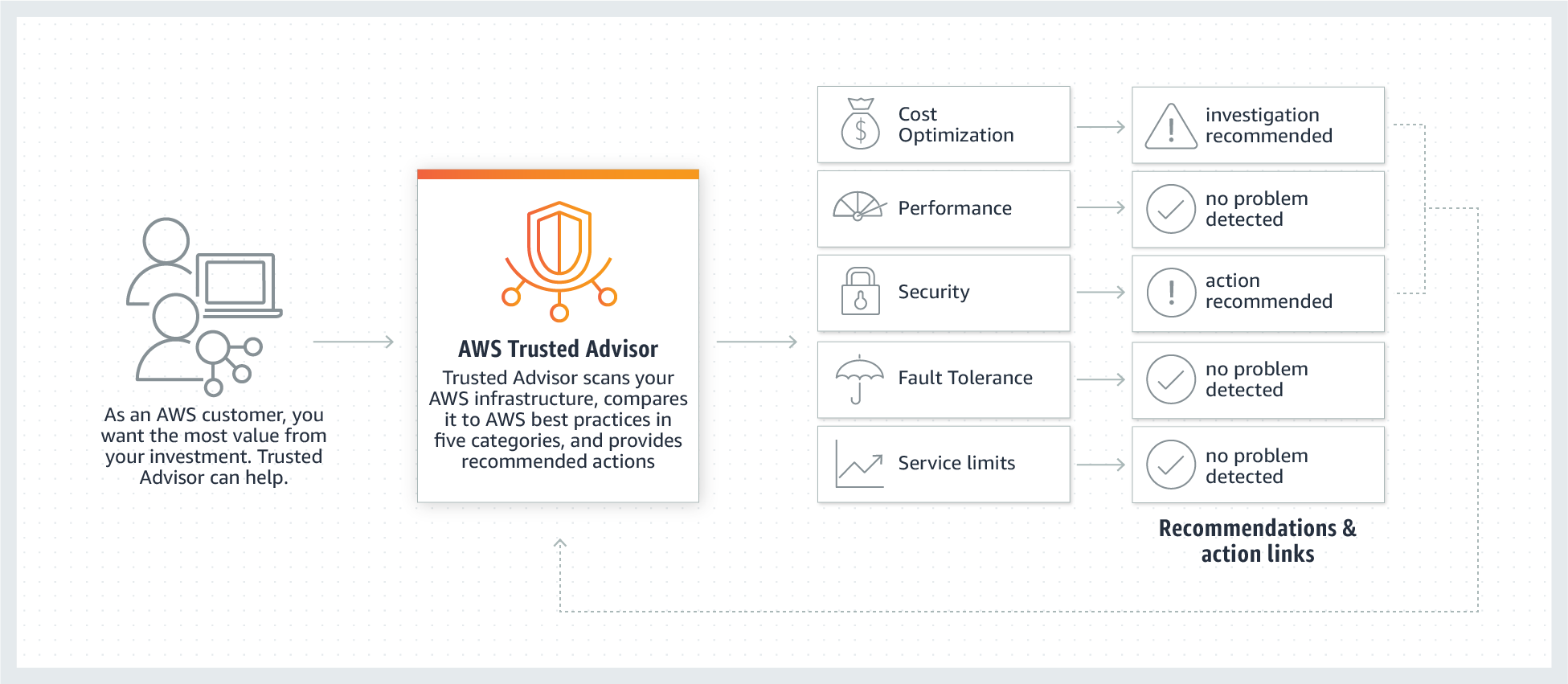
**AWS Trusted Advisor**

AWS Trusted Advisor is an online tool that provides real-time guidance to help provision your resources following AWS best practices. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally. AWS Trusted Advisor analyses your AWS environment and provides best practice recommendations in five categories: Cost Optimization, Performance, Security, Fault Tolerance, Service Limits.

AWS Trusted Advisor can check Amazon Elastic Block Store (Amazon EBS) volume configurations and warns when volumes appear to be underused. Charges begin when a volume is created. If a volume remains unattached or has very low write activity (excluding boot volumes) for a period of time, the volume is probably not being used.

 via - <https://aws.amazon.com/premiumsupport/technology/trusted-advisor/>

**AWS Config** - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Think resource-specific change history, audit, and compliance; think Config. Its a configuration tracking service and not an infrastructure tracking service.

**Amazon CloudWatch** - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. Amazon EBS emits notifications based on Amazon CloudWatch Events for a variety of volume, snapshot, and encryption status changes. With CloudWatch Events, you can establish rules that trigger programmatic actions in response to a change in volume, snapshot, or encryption key state (though not for underutilized volume usage).

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources such as on-premises servers.

**Amazon Inspector** - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. Its a security assessment service and not an infrastructure tracking service.

**AWS Compute Optimizer** helps you identify the optimal AWS resource configurations, such as Amazon EC2 instance types, Amazon EBS volume configurations, and AWS Lambda function memory sizes, using machine learning to analyze historical utilization metrics. AWS Compute Optimizer delivers recommendations for selected types of EC2 instances, EC2 Auto Scaling groups, EBS volumes, and Lambda functions.

Compute Optimizer calculates an individual performance risk score for each resource dimension of the recommended instance, including CPU, memory, EBS throughput, EBS IOPS, disk throughput, disk throughput, network throughput, and network packets per second (PPS).

**AWS CodeDeploy**

AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with your infrastructure so you can easily deploy to one instance or thousands.

**AWS CodeCommit** - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. It cannot be used to automate code deployment.

**AWS CloudFormation** - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all regions and accounts. It cannot be used to automate code deployment.

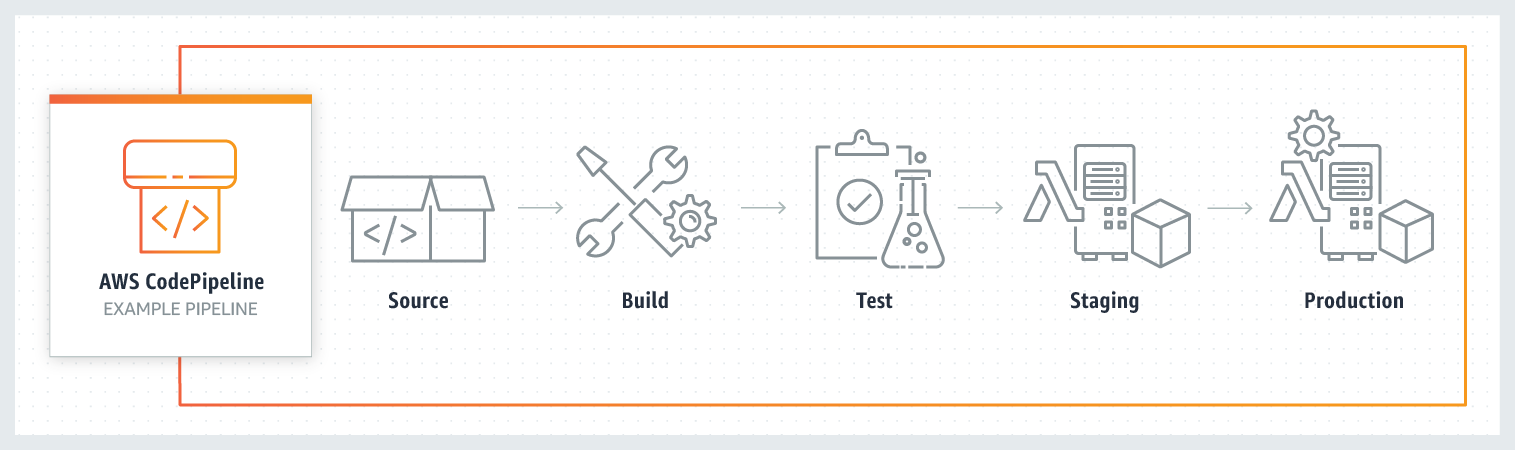
AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

You can use the AWS CloudFormation sample templates or create your own templates to describe your AWS resources, and any associated dependencies or runtime parameters, required to run your application. This provides a single source of truth for all your resources and helps you to standardize infrastructure components used across your organization, enabling configuration compliance and faster troubleshooting.

CloudFormation templates allow you to estimate the cost of your resources.

**AWS CodePipeline** - AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software. With AWS CodePipeline, you model the full release process for building your code, deploying to pre-production environments, testing your application and releasing it to production.

AWS CodePipeline integrates with AWS services such as AWS CodeCommit, Amazon S3, AWS CodeBuild, AWS CodeDeploy, AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon ECS, and AWS Lambda. To further elucidate, CodePipeline cannot by itself deploy the code, it can integrate with CodeDeploy for the actual deployment.



**A VPC peering** connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

**Site to Site VPN** - AWS Site-to-Site VPN creates a secure connection between your on premise data center or branch office and your AWS cloud resources. This connection goes over the public internet. Site to Site VPN cannot be used to interconnect VPCs.

**AWS Direct Connect** - AWS Direct Connect creates a dedicated private connection from a remote network to your VPC. This is a private connection and does not use the public internet. Takes at least a month to establish this connection. Direct Connect cannot be used to interconnect VPCs.

**VPC Endpoint** - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. You cannot connect two VPCs using a VPC endpoint.

**AWS Fargate**

AWS Fargate is a serverless compute engine for containers that works with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS). Fargate makes it easy for you to focus on building your applications. Fargate removes the need to provision and manage servers, lets you specify and pay for resources per application, and improves security through application isolation by design.

**AWS Elastic Beanstalk** - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. You simply upload your code and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring. Beanstalk provisions servers so it is not a serverless service.

**Amazon Simple Notification Service** - Amazon Simple Notification Service (SNS) is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and serverless applications.

**Amazon SageMaker** - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

**AWS Local Zones**

AWS Local Zones allow you to use select AWS services, like compute and storage services, closer to more end-users, providing them very low latency access to the applications running locally. AWS Local Zones are also connected to the parent region via Amazon’s redundant and very high bandwidth private network, giving applications running in AWS Local Zones fast, secure, and seamless access to the rest of AWS services.

You should use AWS Local Zones to deploy workloads closer to your end-users for low-latency requirements. AWS Local Zones have their connection to the internet and support AWS Direct Connect, so resources created in the Local Zone can serve local end-users with very low-latency communications.

**AWS Edge Locations** - An AWS Edge location is a site that CloudFront uses to cache copies of the content for faster delivery to users at any location.

**AWS Wavelength** - AWS Wavelength extends the AWS cloud to a global network of 5G edge locations to enable developers to innovate and build a whole new class of applications that require ultra-low latency. Wavelength Zones provide a high-bandwidth, secure connection to the parent AWS Region, allowing developers to seamlessly connect to the full range of services in the AWS Region through the same APIs and toolsets.

**AWS Direct Connect** - AWS Direct Connect is a cloud service that links your network directly to AWS, bypassing the internet to deliver more consistent, lower-latency performance. When creating a new connection, you can choose a hosted connection provided by an AWS Direct Connect Delivery Partner, or choose a dedicated connection from AWS—and deploy at over 100 AWS Direct Connect locations around the world. AWS Direct Connect provides consistently high bandwidth, low-latency access and it is generally used between on-premises data centers and AWS network. Direct Connect is overkill for the given requirement.

**Auto Scaling**

Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size.

**Multi AZ deployment** - With Availability Zones, you can design and operate applications and databases that automatically failover between zones without interruption. Multi AZ deployment of EC2 instances provided high availability, it does not help in scaling resources.

**Network Load Balancer** - Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Transport Layer Security (TLS) traffic where extreme performance is required. It distributes traffic, does not scale resources.

**Application Load Balancer** - An Application Load Balancer serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. It distributes traffic, does not scale resources.

**AWS Trusted Advisor** is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on cost optimization, security, fault tolerance, service limits, and performance improvement. Whether establishing new workflows, developing applications, or as part of ongoing improvement, recommendations provided by Trusted Advisor regularly help keep your solutions provisioned optimally.

**Service Quotas** enables you to view and manage your quotas for AWS services from a central location. Quotas, also referred to as limits in AWS, are the maximum values for the resources, actions, and items in your AWS account. Each AWS service defines its quotas and establishes default values for those quotas.

**APN Consulting Partner**

The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers.

APN Consulting Partners are professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their migration to AWS cloud.

**APN Technology Partner** - APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on or integrated with, the AWS Cloud. APN Technology Partners cannot help in migrating to AWS and managing applications on AWS Cloud.

**Concierge Support Team** - The Concierge Support Team are AWS billing and account experts that specialize in working with enterprise accounts. They will quickly and efficiently assist you with your billing and account inquiries. The Concierge Support Team is only available for the Enterprise Support plan. Concierge Support Team cannot help in migrating to AWS and managing applications on AWS Cloud.

**You must use an AMI from the same region as that of the EC2 instance. The region of the AMI has no bearing on the performance of the EC2 instance**

**AWS Directory Service** - AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. It is not used to deploy resources.

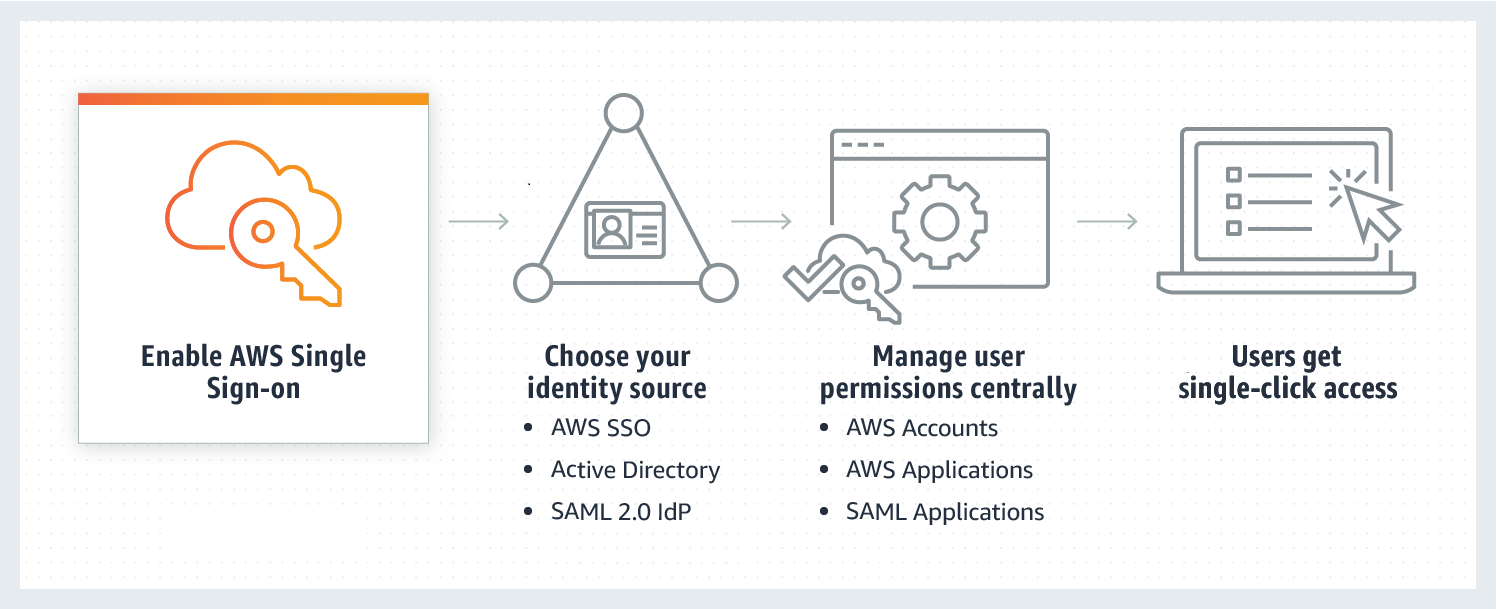
**Amazon LightSail** - Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. It is not best suited when deploying more complex resources, while CloudFormation can.

**AWS CodeDeploy** - AWS CodeDeploy is a service that automates code deployments to any instance, including EC2 instances and instances running on-premises. Unlike CloudFormation, it does not deal with infrastructure configuration and orchestration.

**AWS Single Sign-On (SSO)**

AWS SSO is an AWS service that enables you to makes it easy to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place.

With AWS SSO, you can easily manage SSO access and user permissions to all of your accounts in AWS Organizations centrally. AWS SSO allows you to create and manage user identities in AWS SSO’s identity store, or easily connect to your existing identity source including Microsoft Active Directory, Azure Active Directory (Azure AD), and Okta Universal Directory.

You can use AWS SSO to quickly and easily assign and manage your employees’ access to multiple AWS accounts, SAML-enabled cloud applications (such as Salesforce, Office 365, and Box), and custom-built in-house applications, all from a central place.  via - <https://aws.amazon.com/single-sign-on/>

**AWS Cognito** - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. With Amazon Cognito, you also have the option to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using your own identity system. It is an identity management solution for customers/developers building B2C or B2B apps for their customers.

**AWS Identity and Access Management (IAM)** - AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. It is not used to log in but to manage users and roles.

**AWS Command Line Interface (CLI)** - The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts. It is not a central user portal.

**Penetration Testing**

AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services. Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves.

**Network Stress Testing** - AWS considers "network stress test" to be when a test sends a large volume of legitimate or test traffic to a specific intended target application. The endpoint and infrastructure are expected to be able to handle this traffic.

**Amazon Inspector** - Amazon Inspector is an automated, security assessment service that helps you check for unintended network accessibility of your Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as pre-defined rules packages mapped to common security best practices and vulnerability definitions.

**AWS Secrets Manager** - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

**AWS Organizations** helps you centrally govern your environment as you grow and scale your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts.

Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance. You can also simplify billing by setting up a single payment method for all of your AWS accounts. Through integrations with other AWS services, you can use Organizations to define central configurations and resource sharing across accounts in your organization. AWS Organizations is available to all AWS customers at no additional charge.

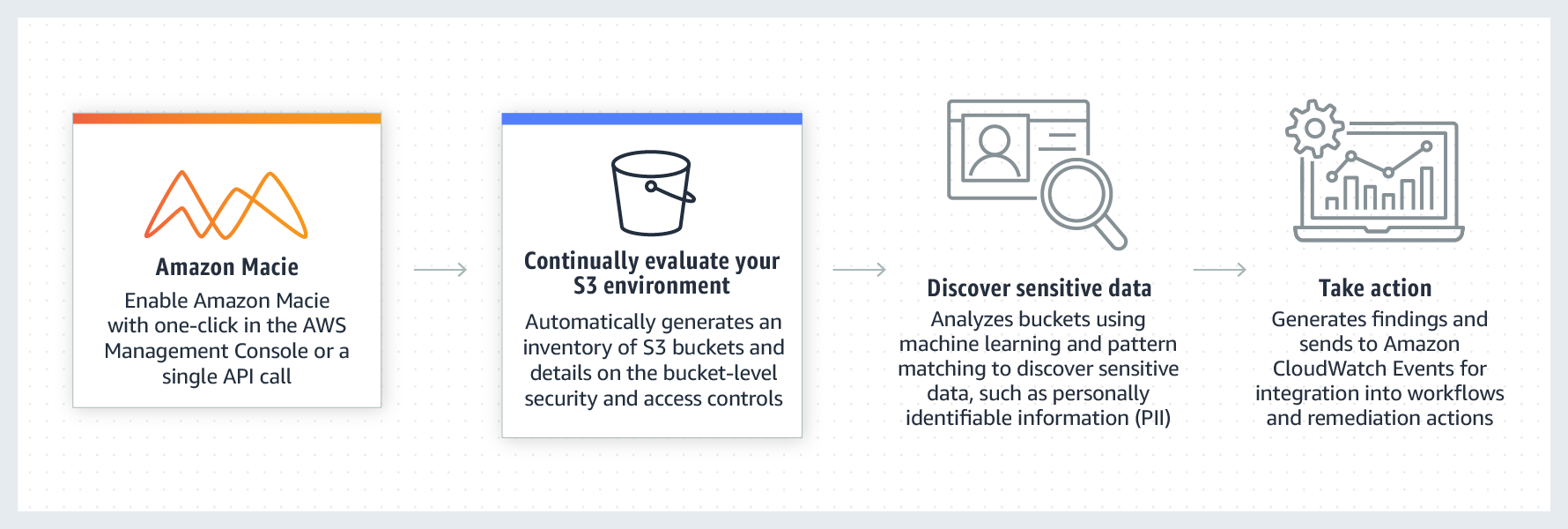
You should create accounts per department based on regulatory restrictions (using SCP) for better resource isolation, and to have separate per-account service limits.

AWS Organizations allows you to restrict what services and actions are allowed in your accounts. You can use Service Control Policies (SCPs) to apply permission guardrails on AWS Identity and Access Management (IAM) users and roles.

- You should use tags standards to categorize AWS resources for billing purposes.

- You should enable CloudTrail to monitor activity on all accounts for governance, compliance, risk, and auditing purposes.

- AWS Organizations helps you simplify IT operations by automating AWS account creation and management. The Organizations APIs enable you to create new accounts programmatically, and to add the new accounts to a group. The policies attached to the group are automatically applied to the new account.

**Amazon Macie** - Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those you have defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets you select to identify and alert you to sensitive data, such as personally identifiable information (PII). via - <https://aws.amazon.com/macie/>

**AWS Glue** - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. AWS Glue job is meant to be used for batch ETL data processing. It cannot be used to discover and protect your sensitive data in AWS.

**Amazon Polly** - Amazon Polly is a service that turns text into lifelike speech, allowing you to create applications that talk, and build entirely new categories of speech-enabled products. Polly's Text-to-Speech (TTS) service uses advanced deep learning technologies to synthesize natural sounding human speech. It cannot be used to discover and protect your sensitive data in AWS.

**AWS Pricing Calculator**

AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services. AWS Pricing Calculator can be accessed at <https://calculator.aws/#/>.

AWS also offers a complimentary service called Migration Evaluator (Formerly TSO Logic) to create data-driven business cases for AWS Cloud planning and migration.

**AWS Cost Explorer** - AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost Explorer includes a default report that helps you visualize the costs and usage associated with your top five cost-accruing AWS services, and gives you a detailed breakdown of all services in the table view. The reports let you adjust the time range to view historical data going back up to twelve months to gain an understanding of your cost trends. AWS Cost Explorer cannot be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

**AWS Budgets** - AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. You can also use AWS Budgets to set reservation utilization or coverage targets and receive alerts when your utilization drops below the threshold you define. Budgets can be created at the monthly, quarterly, or yearly level, and you can customize the start and end dates. You can further refine your budget to track costs associated with multiple dimensions, such as AWS service, linked account, tag, and others. AWS Budgets cannot be used to compare the cost of running the IT infrastructure on-premises vs AWS Cloud.

**AWS OpsWorks**

OpsWorks lets you use Chef and Puppet to automate how servers are configured, deployed, and managed across your Amazon EC2 instances or on-premises compute environments.

**AWS Batch** - AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.

**AWS CloudHSM**

AWS CloudHSM is a cloud-based Hardware Security Module (HSM) that enables you to easily generate and use your encryption keys on the AWS Cloud. With CloudHSM, you can manage your encryption keys using FIPS 140-2 Level 3 validated HSMs. It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.

**AWS Systems Session Manager**

AWS SSM Session Manager is a fully-managed service that provides you with an interactive browser-based shell and CLI experience. It helps provide secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, and manage SSH keys. Session Manager helps to enable compliance with corporate policies that require controlled access to instances, increase security and auditability of access to the instances while providing simplicity and cross-platform instance access to end-users.

**AWS Storage Gateway** - AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. All data transferred between the gateway and AWS storage is encrypted using SSL (for all three types of gateways - File, Volume and Tape Gateways). Storage Gateway cannot be used for data archival.

**AWS Quick Starts references**

Quick Starts are built by AWS solutions architects and partners to help you deploy popular technologies on AWS, based on AWS best practices for security and high availability. These accelerators reduce hundreds of manual procedures into just a few steps, so you can build your production environment quickly and start using it immediately.

Each Quick Start includes AWS CloudFormation templates that automate the deployment and a guide that discusses the architecture and provides step-by-step deployment instructions.

**Step Function** - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. You can design and run workflows that stitch together services such as AWS Lambda, AWS Glue and Amazon SageMaker. Step Function cannot be used to run a process on a schedule.