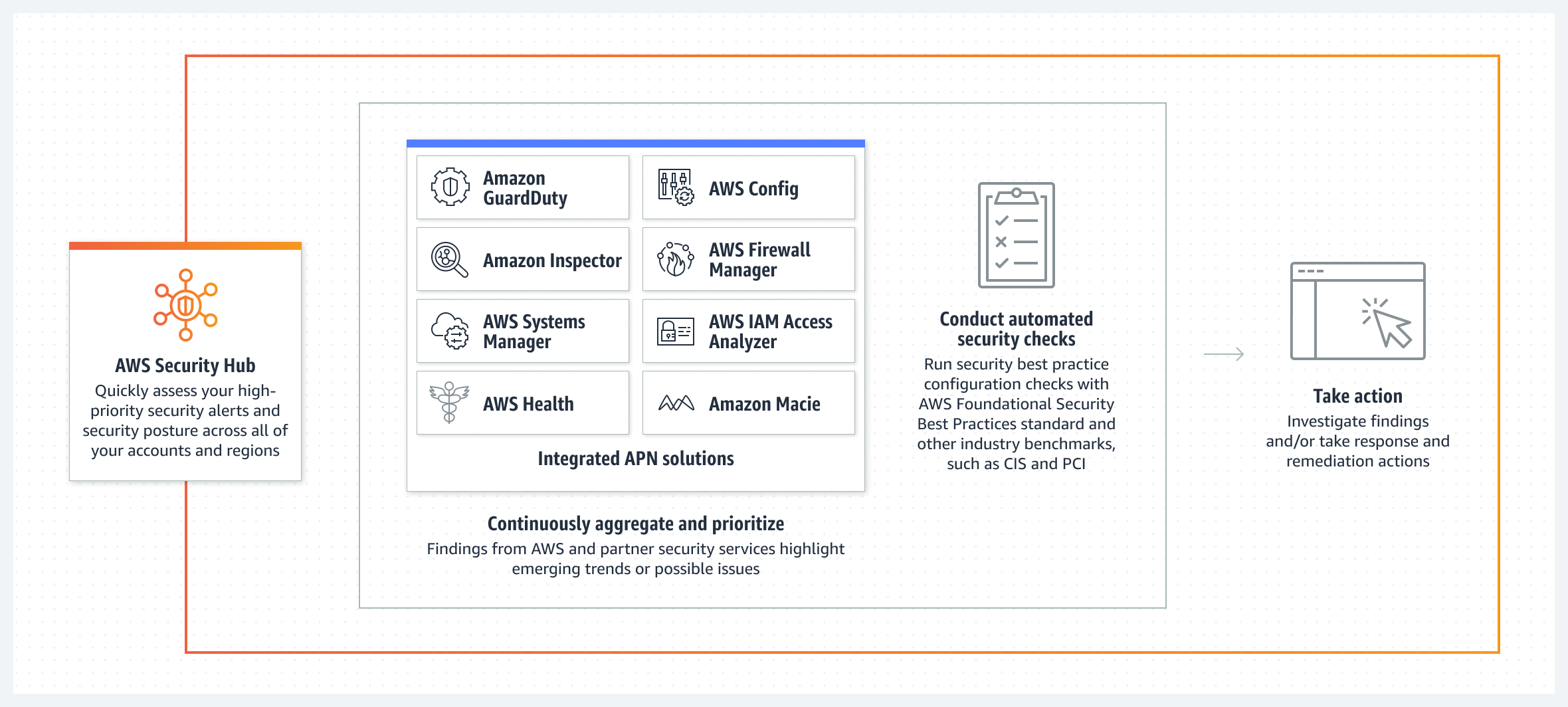
**What is AWS Security Hub**

Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

AWS Security Hub is a service provided by Amazon Web Services (AWS) that helps you keep your AWS accounts secure. It brings together information about security issues from different sources and gives you a single place to monitor and manage them.

**Working**

****

**Benefits:**

**Reduce the time and effort to collect information**

**Best practices and standards security checks**

**Consolidated view across AWS accounts**

**Some Key Features**

* **Aggregated Security Alerts**
* **Continuous Security Monitoring**
* Recommendations
* Integration with AWS Organization

**Amazon GuardDuty**

GuardDuty will continuously monitor our “AWS accounts, workloads and data stored in Amazon S3” and alert us when there is a potential threat.

**Amazon Inspector**

AWS inspector finds security vulnerabilities for EC2 instances.

**AWS System Manager**

AWS System Manager is an AWS service that we can use to view and control our infrastructure on AWS.

**AWS Health**

AWS Health provides customers with a centralized view of the health of their AWS resources and services, allowing them to stay informed about events that can affect their account and services.

**AWS config**

AWS Config provides customers with a detailed view of the resources associated with their AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

**AWS Firewall Manager**

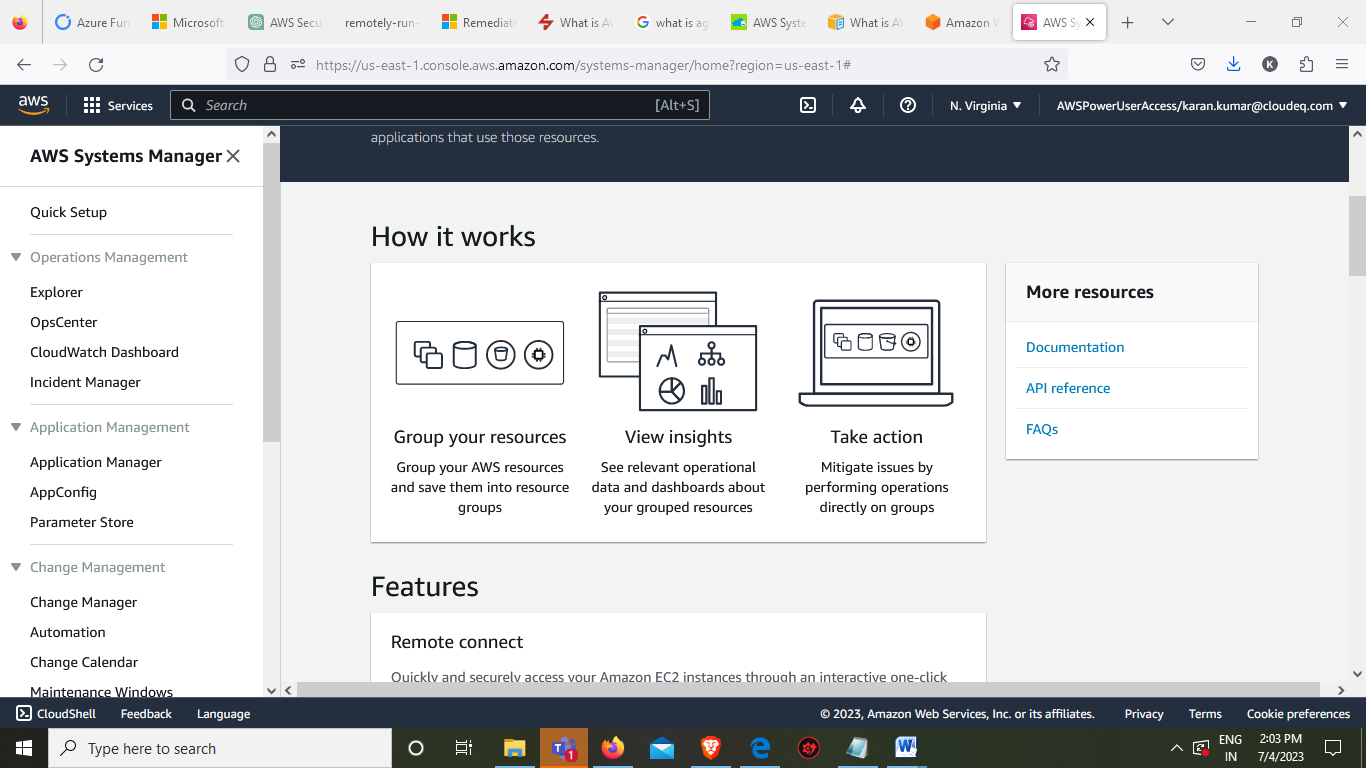
AWS Firewall Manager provides customers with a centralized and automated way to manage firewall rules and enforce security policies across their AWS accounts and resources, helping to ensure compliance and reduce risk.

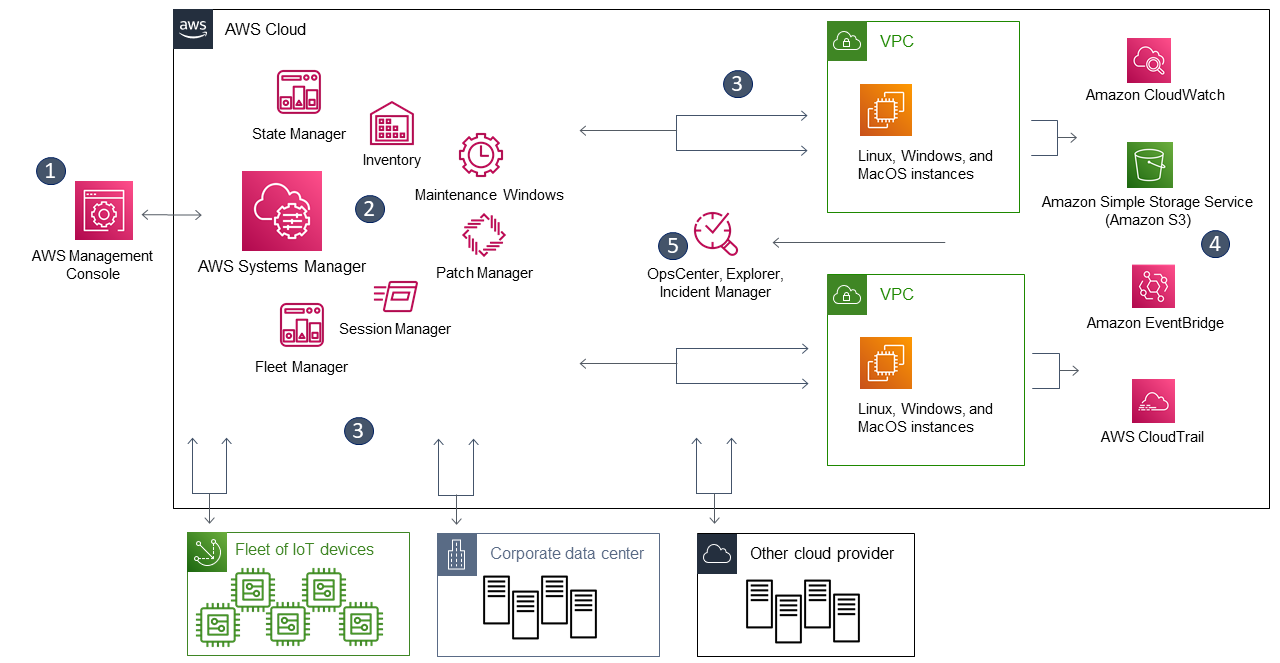
**AWS IAM Access Analyzer**

AWS IAM Access Analyzer provides customers with a way to identify potential resource-access risks by analyzing resource-based policies in their AWS environment, helping to ensure compliance and reduce risk

**What is AWS System Manager**

Aws system manger is a aws service that you can use to view a and control your infrastructure on aws. System Manager helps you maintain security and compliance by scanning your managed instance and reporting on any policy violation it detects.



****

**Features**

* Remote Connect
* Resource Grouping
* Insight and Dashboard
* Remote execution
* Maintenance Windows
* Software inventory

**What is AWS Session Manager**

It is fully managed resource provided by AWS that allow us to manage, access and troubleshoot our EC2 instance. Session manager provides us the secure instance management without need to open inbound port and manage SSH key to quickly and securely access our windows and linux instance.

Session Manager is a feature on AWS that allows you to connect to your machines without opening ports. On Linux machines, we can execute commands in the console via the browser, let me emphasize this again **without opening any ports, even ssh**.

## What are the main features of Session Manager?

* Support for Windows Server, Linux and macOS managed nodes
* IAM access control
* Tunneling
* Interactive commands